ViOnyx Web Server
GUÍA DE USUARIO DE

Versión 1.1.0

Español
ES 102.00.VQF12-R

suprema
SECURITY & BIOMETRICS

CONTENIDO

Primeros Pasos 5

Instalación del certificado 5

Establecer contraseña 10

Iniciar sesión 11

Comprender la Interfaz de Usuario 13

Acceso rápido al menú principal 13

Información y herramientas 14

Ver en Vivo 15

Diseño básico de la vista en vivo 15

Seleccione canal y modo de visualización 15

Acercamiento 16

Rotar la pantalla 17

Captura de pantalla 17

Modo de pantalla completa 18

Opciones de visualización de IA 18

Abra el panel Face Shot 19

Cuando el video no se reproduce 20

Administrar Eventos de IA 21

Configurar Eventos de Seguimiento de Personas 21

Configurar Eventos de Detección de Intrusión 29

Configurar Evento de Detección de Cruce de Línea 36

Configurar Evento de Conteo de Personas 43

Configurar Eventos De Control De Acceso 50

Editar y Eliminar Eventos de IA 60

Ajustes de Reglas de IA 61

Administrar horarios 68

Configuración Avanzada 72

Configurar la Cámara 75

Configurar Perfil de Video 75

Configurar Ajustes de la Cámara 78

Configurar Ajustes de Privacidad y Superposición 82

Configurar Fecha y Hora 86

Configurar Ajustes de Red 88

Configurar RS-485 99

Integrar RTSP y ONVIF 107

Administrar Usuarios 110

Configurar Autenticación Facial 110

Agregar usuarios 110

Editar y Eliminar Usuarios 117

Búsqueda y Vista de Usuarios 120

Administrar Control De Acceso 124

Administrar Puertas 124

Administrar Niveles de Acceso 130

Controlar Puertas 136

Configurar Reglas de Puerta 138

Configurar Sistema 146

Actualizar Información de la Cámara 146

Actualizar Firmware 148

Mantener la Cámara 150

Subir Clips de Audio 154

Actualizar Contraseña de la Cuenta de Administrador 156

Administrar Operadores 158

Ver Registros del Sistema 163

Tipos de Registros del Sistema 168

Apéndices 177

Descargos de responsabilidad 177

Aviso de derechos de autor 178

Primeros Pasos

Después de instalar la cámara ViOnyx, complete la configuración inicial en un navegador web. Este documento explica todos los pasos necesarios, desde la instalación del certificado hasta la configuración de la contraseña del administrador y el inicio de sesión.

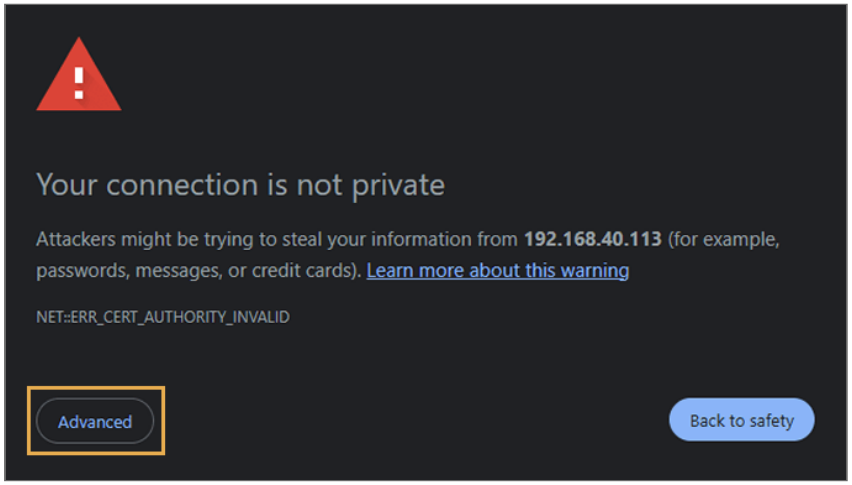
> **Información**
> Si la cámara no obtiene una dirección IP después de un restablecimiento de fábrica, cambia a la dirección IP predeterminada (`https://192.168.1.100`). Conéctese a esa dirección en su navegador web.

Instalación del certificado

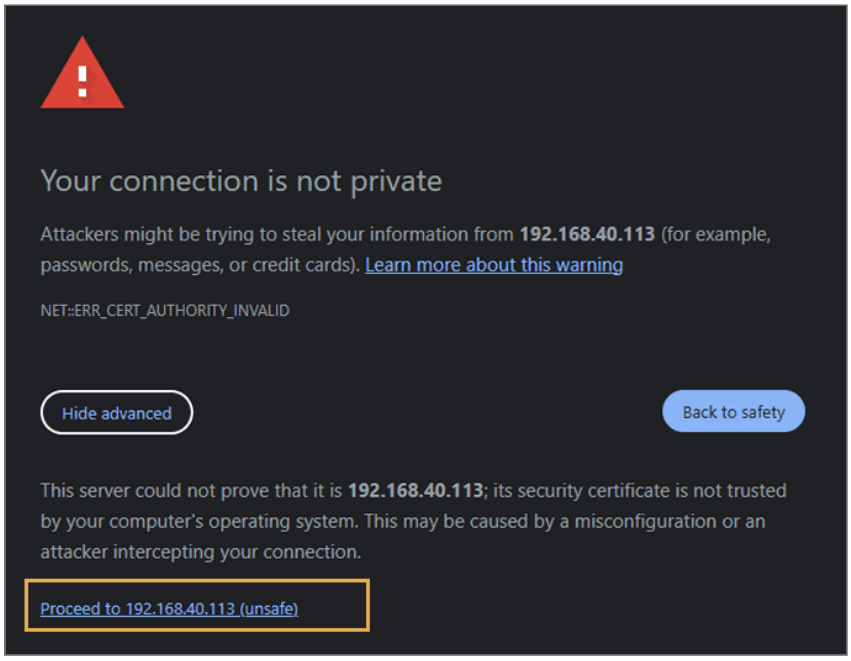
ViOnyx Web Server usa una conexión HTTPS segura. Aparece una advertencia de seguridad la primera vez que se conecta porque la cámara usa un certificado autofirmado. Aprenda a conectarse al servidor web de forma segura sin advertencias después de agregar el certificado al almacén de confianza de Windows.

1 Descargar certificado

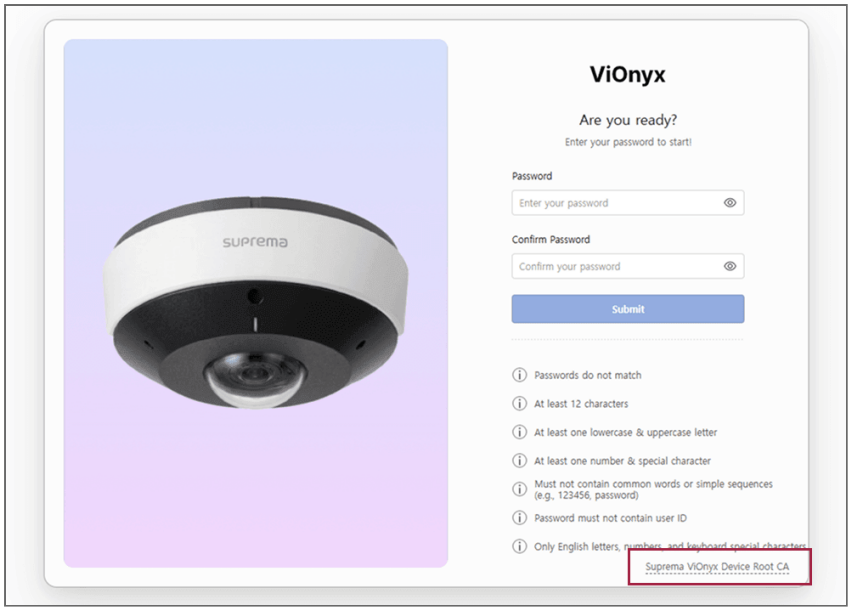
1. Conéctese a la cámara en su navegador web usando la dirección IP asignada (`https://{IP_address}`).
2. Si aparece el mensaje de advertencia "**Your connection is not private**", haga clic en **Advanced** en la parte inferior.



3. Despliegue la sección **Advanced** y luego haga clic en **Proceed to** `https://{IP_address}` **(unsafe)** o en un vínculo similar para continuar.



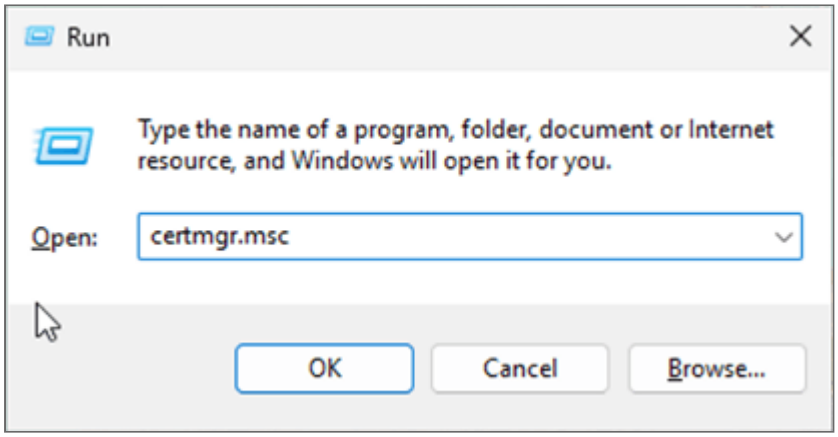
4. Haga clic en el enlace **Suprema ViOnyx Device Root CA** en la parte inferior de la pantalla de configuración de la contraseña.



5. Guarde localmente el archivo de certificado `Suprema_ViOnyx_Device_{serial-number}_Root_CA.crt`.

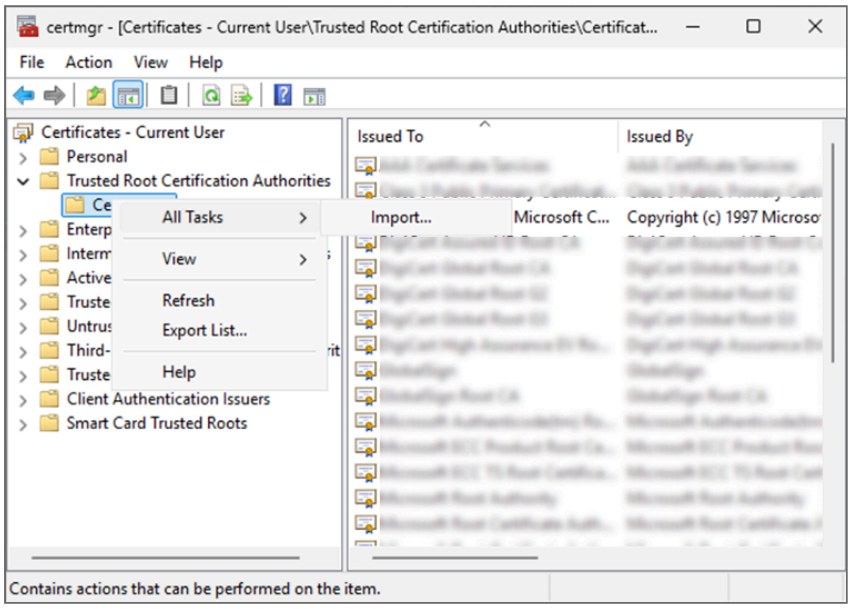
2 Abra la consola de administración de Windows

1. Presione Inicio + `R` para abrir la ventana Ejecutar.
2. Escriba `certmgr.msc` y luego presione `Enter` para abrir la **Management Console**.

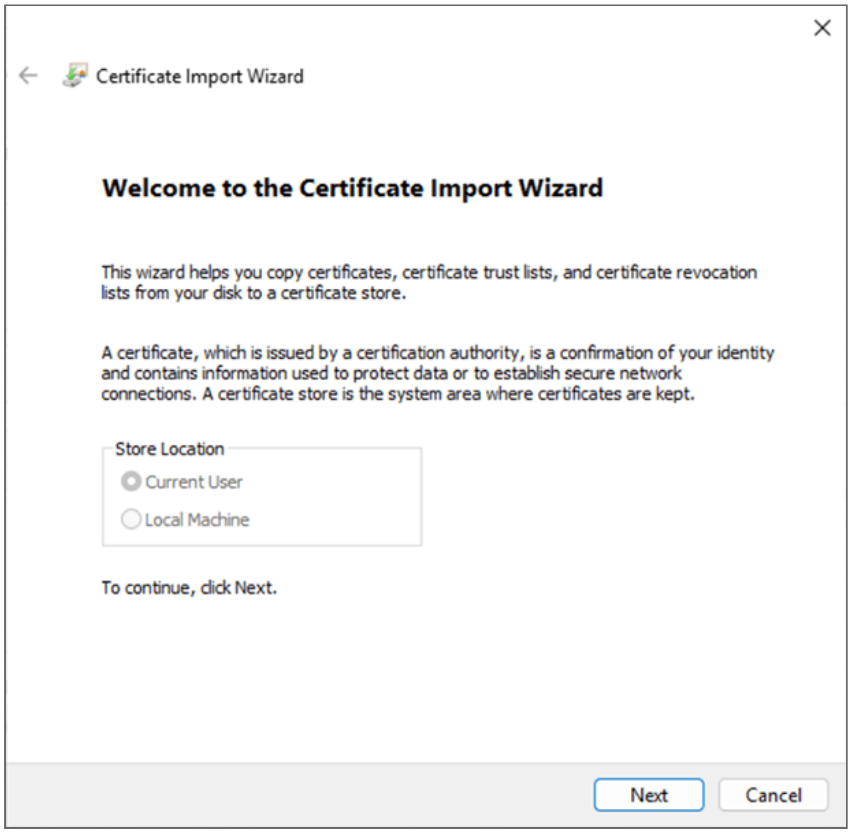


3 Ejecute el asistente de importación de certificados

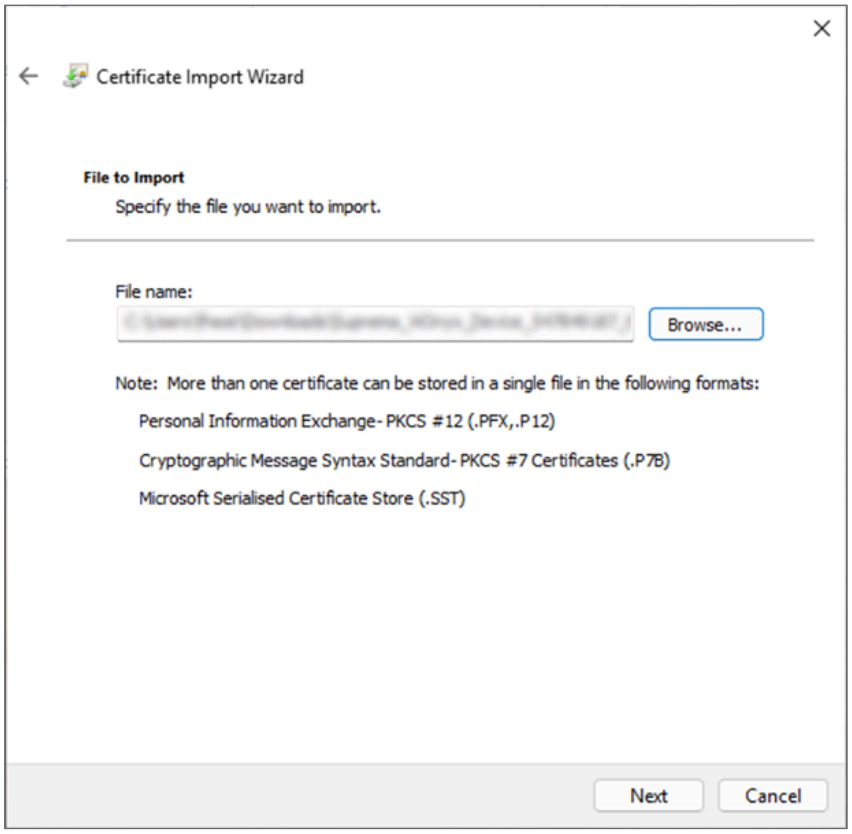
1. En el panel izquierdo de la **Consola de administración**, expanda **Entidades de certificación raíz de confianza**.
2. Haga clic derecho en **Certificates** debajo de esta opción y luego seleccione **All Tasks** → **Import**.



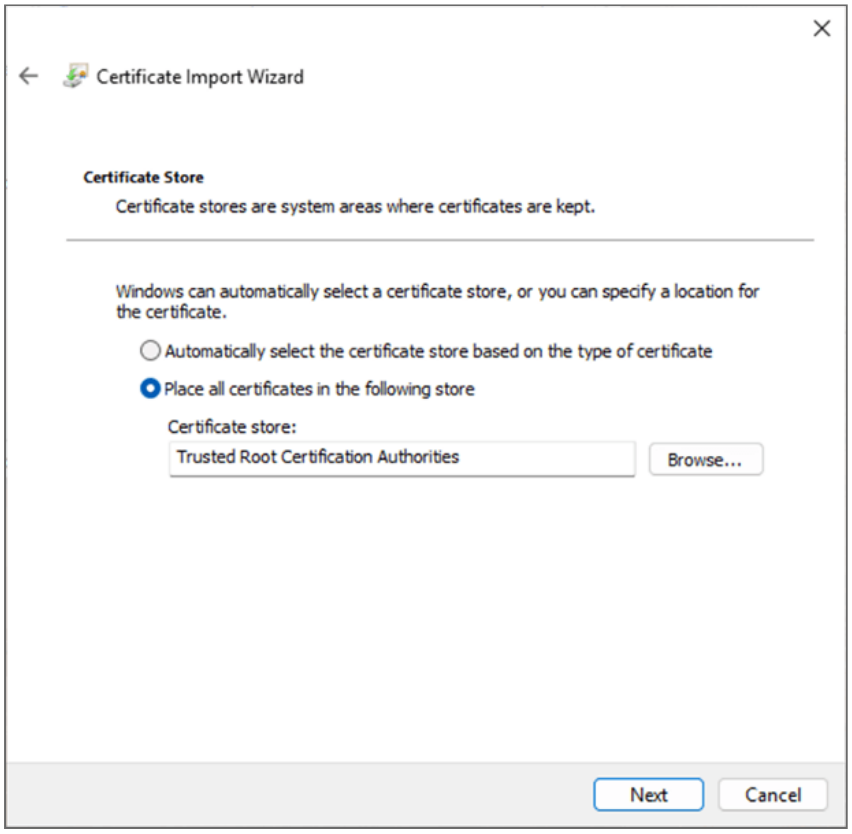
3. En el Asistente para importación de certificados, haga clic en **Next**.



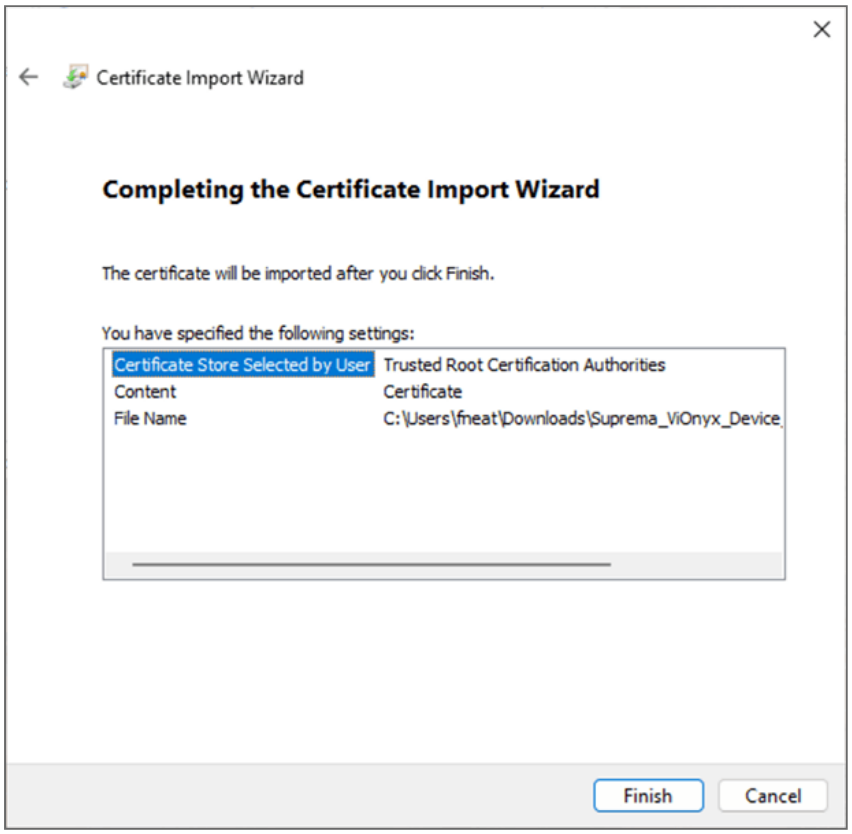
4. Haga clic en **Browse** y seleccione el archivo de certificado guardado `Suprema_ViOnyx_Device_547849187_Root_CA.crt`.



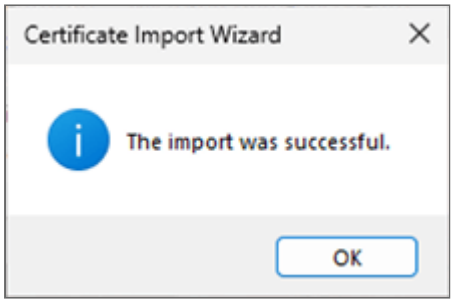
5. Haga clic en **Next**.
6. Seleccione **Place all certificates in the following store**.
7. Asegúrese de que **Certificate store** esté configurado en **Trusted Root Certification Authorities**.



8. Haga clic en **Next**.
9. Haga clic en **Finish** para completar la importación del certificado.

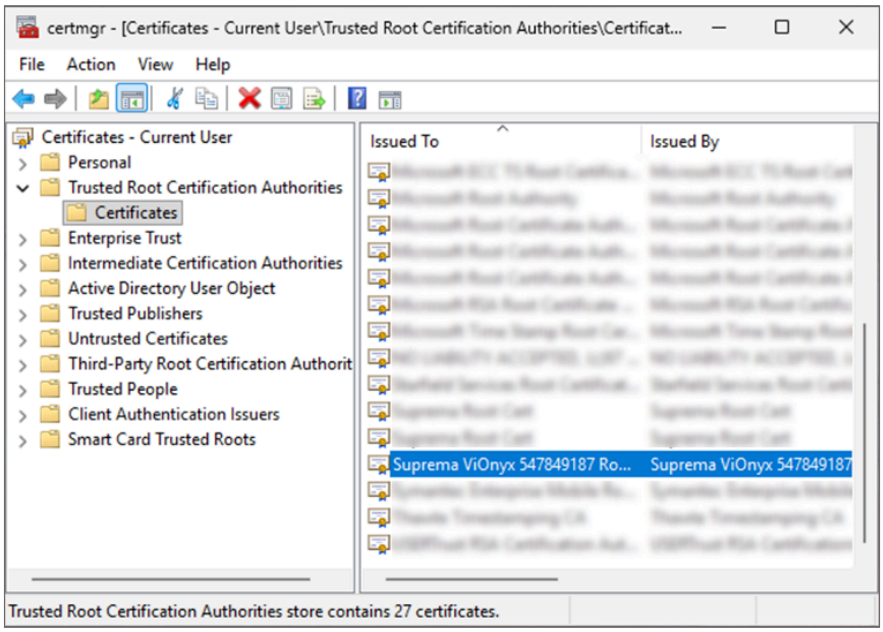


10. Si aparece una advertencia de seguridad, haga clic en **Yes**.
11. Cuando aparezca el mensaje de importación correcta del certificado, haga clic en **OK**.



4 Verificar la instalación del certificado

En la **Management Console**, seleccione **Trusted Root Certification Authorities** → **Certificates** para confirmar que el certificado importado aparezca en la lista.

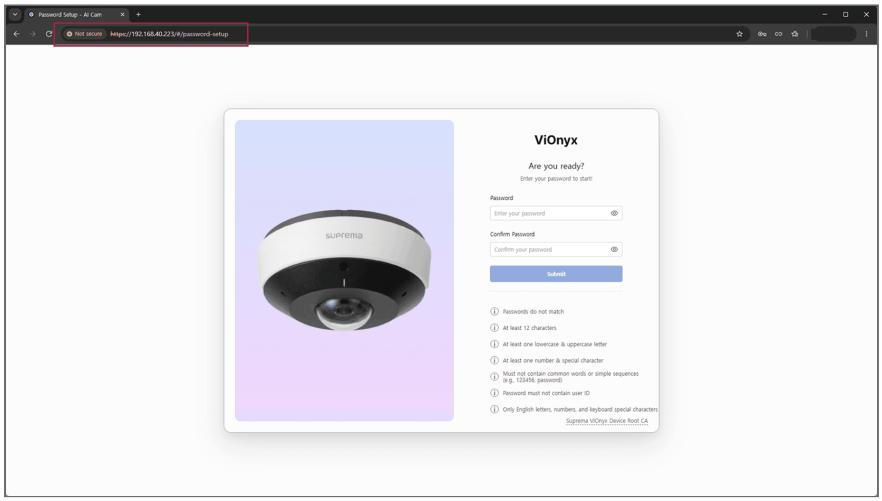


Después de completar la instalación del certificado, cierre por completo y reinicie el navegador web, y luego vuelva a conectarse usando la dirección IP de la cámara. Ahora se conecta de forma segura sin una advertencia de seguridad.

Establecer contraseña

Configure una contraseña segura por seguridad al iniciar sesión por primera vez. ViOnyx aplica una política de contraseñas seguras para proteger la seguridad del sistema.

1. Conéctese a la cámara en su navegador web usando la dirección IP asignada (`https://{IP_address}`).



2. En la página de configuración de la contraseña, introduzca una nueva contraseña en el campo de entrada **Password**.
3. Vuelva a introducir la misma contraseña en el campo **Confirm Password**.
4. Asegúrese de que la contraseña que introdujo cumpla con todos los siguientes requisitos.
5. Cuando se cumplan todas las condiciones, **Submit** se activa. Haga clic en el botón para finalizar la configuración de su contraseña.

Requisitos de la contraseña

La contraseña debe cumplir con todos los requisitos siguientes:

- Los valores de los campos **Password** y **Confirm Password** deben coincidir exactamente.
- La contraseña debe tener al menos 12 caracteres. Longitud máxima: 64 caracteres.
- Incluya al menos una letra minúscula (`a-z`) y una mayúscula (`A-Z`).
- Incluya al menos un dígito (`0-9`) y un carácter especial.

  > *Ejemplos de caracteres especiales:* `"` `!` `@` `#` `$` `%` `^` `&` `*` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}`

- No incluya secuencias de 4 o más caracteres consecutivos (por ejemplo, `1234` , `abcd`) ni 4 o más caracteres idénticos.
- El nombre de usuario (sin distinguir mayúsculas y minúsculas) no debe incluirse en la contraseña.

  > *admin, Admin, ADMIN, Admin123! etc.*

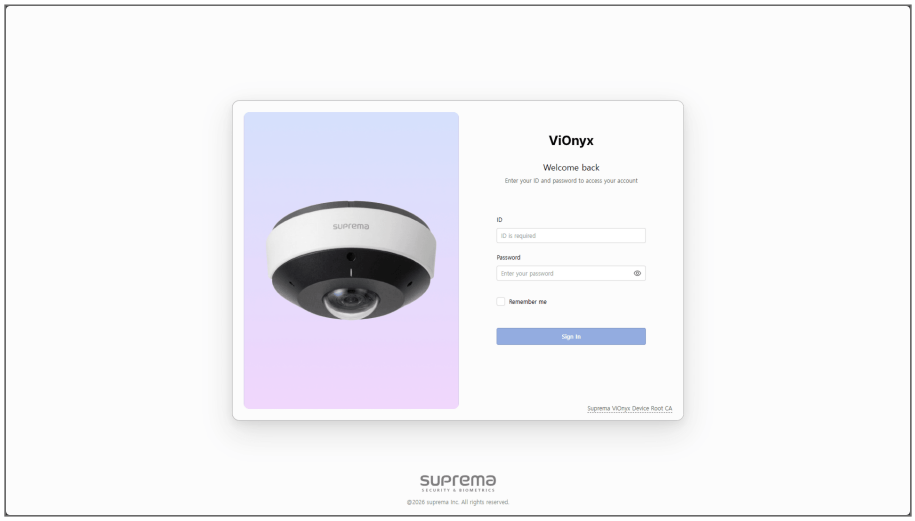
- No se permiten contraseñas débiles comunes como `password` , `qwerty` , `123456` .
- Use solo letras del alfabeto inglés, números y caracteres especiales de un teclado con distribución en inglés.

Precaución

Guarde la contraseña que configuró en un lugar seguro. Si pierde la contraseña, inicialice la cámara.

Iniciar sesión

Después de configurar la contraseña, se le redirigirá automáticamente a la página de inicio de sesión. Introduzca el ID del administrador y la contraseña que configuró para acceder a ViOnyx Web Server.



1. Introduzca **admin** en el campo de entrada **ID**.
2. Introduzca la contraseña que configuró en el campo de entrada **Password**.
3. Haga clic en **Sign In**.

Después de iniciar sesión correctamente, ViOnyx Web Server abre la página **Live**.

> **Información**
> Cambie el ID del administrador (admin) en **System** → **Account**.

Siguiente paso

Explica las principales características y el uso del menú **Live**.
Configure eventos de IA para supervisar situaciones específicas detectadas por la cámara.
Use la configuración de la cámara para mantener una calidad de imagen óptima para el entorno de captura, configurar la red y aplicar políticas de seguridad y privacidad.
Enrolle usuarios para habilitar la feature de reconocimiento facial con IA.
Administra de forma sistemática la información del dispositivo, el firmware, el mantenimiento, las cuentas, el audio y los registros para operar eficazmente el sistema de cámaras.

Comprender la Interfaz de Usuario

Después de iniciar sesión en ViOnyx Web Server, el menú principal aparece en la parte superior. Los menús brindan acceso rápido a las features. Esta página explica la estructura de la interfaz del servidor web y la función de cada menú.



Acceso rápido al menú principal

En la parte superior izquierda aparecen el logotipo de ViOnyx Web Server y los íconos del menú principal. Las features que ofrece cada menú se enumeran a continuación.

Ícono del menú	Nombre del menú	Descripción
	Live	Ver video en vivo de la cámara.
	Settings	Cambie la cámara y las setting del servidor web.
	AI&Rule	Configure eventos y reglas de IA.
	People	Agregue y administre usuarios del sistema de cámaras.
	Access	Vincule puertas, niveles de acceso y permisos de usuario para administrar el control de acceso. Este menú está en beta.
	System	Administre la información del dispositivo, las cuentas, el audio, los registros y otras setting del sistema.

Información

La versión de firmware 1.1.0 o posterior incluye soporte para el menú **Access**.

Información y herramientas

En la parte superior derecha aparecen la información de la cámara, la selección de idioma, un acceso directo a la guía del usuario y un botón para cerrar sesión.

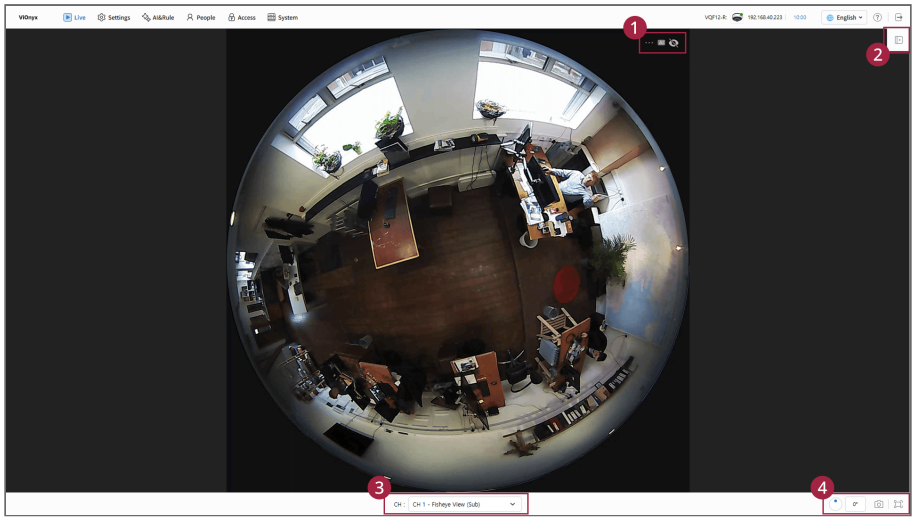
Ícono del menú	Nombre del menú	Descripción
	Información de la cámara	Vea el nombre, el estado y la dirección IP de la cámara conectada. Haga clic en **Dirección IP** para ver la información del dispositivo.
10:00	Tiempo de sesión	Vea el tiempo de sesión del administrador que inició sesión actualmente. Se cierra sesión automáticamente cuando se supera el tiempo de sesión.
	Selección de idioma	Cambie el idioma de la interfaz web.
	Acceso directo a la guía del usuario	Vea la guía del usuario.
	Cerrar sesión	Cerrar sesión.

Ver en Vivo

Use el menú **Live** de ViOnyx Web Server para ver el video en vivo de la cámara. Seleccione el canal y el modo de visualización deseados, luego acerque o vea en pantalla completa.

Diseño básico de la vista en vivo

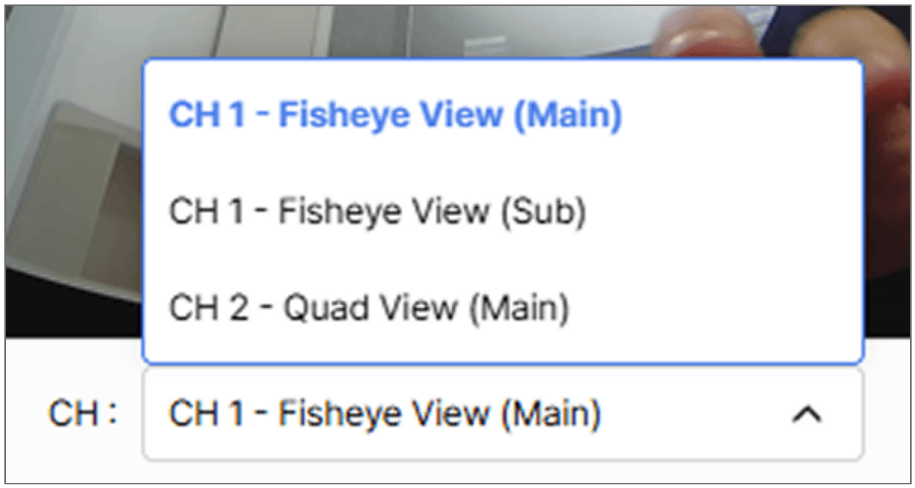
Al entrar por primera vez al menú **Live**, el video aparece en el siguiente estado predeterminado.



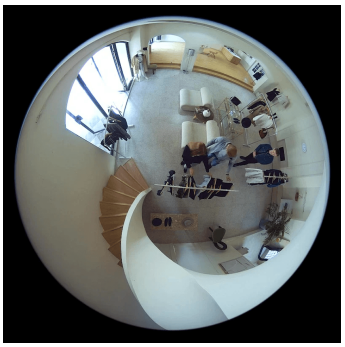
Ítem	Componente	Descripción
1	AI	- Las funciones de IA están deshabilitadas. Haga clic en el icono para habilitar las funciones de IA. - Haga clic en ••• y ajuste la configuración para mostrar u ocultar eventos de IA y cuadros de usuario.
2		Abra el panel **Face Shot**(Face Shot).
3	CH	Seleccione el modo de visualización disponible para cada canal.
4		Gire el video en vivo.
		Capture el video en vivo.
		Vea el video en vivo en pantalla completa.

Seleccione canal y modo de visualización

ViOnyx Web Server ofrece varios canales y modos de visualización. Seleccione el canal y el modo de visualización deseados en la lista desplegable **CH** en la parte inferior de la pantalla.



Canales y modos de visualización compatibles

Canal	Modo de visualización	Descripción	Ejemplo
1ch	Fisheye View (Main/Sub)	Video original de lente ojo de pez para el canal principal	
2ch	Quad View (Main)	Vista dividida en 4 para el canal panorámico	

Información

- Los flujos Principal y Secundario de cada canal ofrecen diferentes resoluciones. Principal es el flujo de mayor calidad; Secundario es el flujo de menor calidad.
- La imagen es una pantalla de ejemplo. La pantalla real puede diferir.

Acercamiento

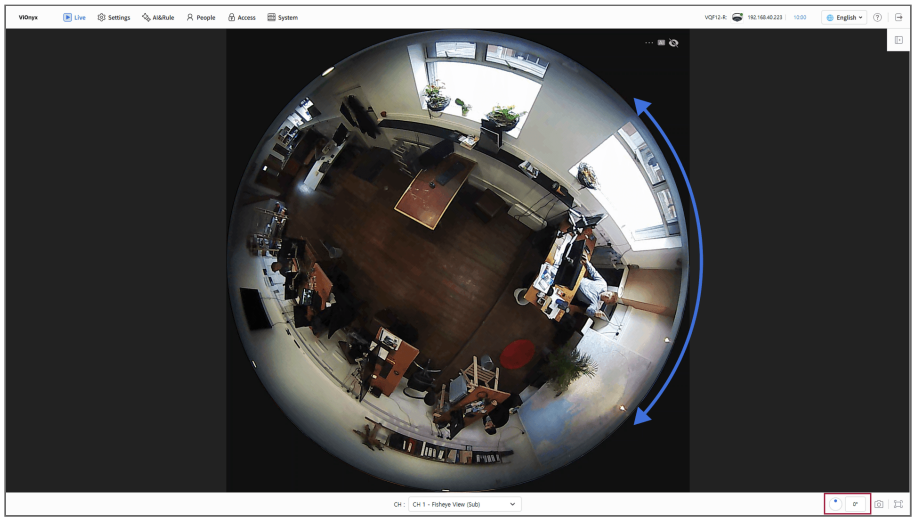
Use el mouse para acercar y alejar.

- Desplazar hacia arriba: acercar
- Desplazar hacia abajo: alejar
- Doble clic: regresar al tamaño original (1x)

> **Información**
>
> - Rango de zoom: 1x ~ 8x.
> - El acercamiento usa ampliación digital, por lo que la imagen puede verse borrosa con niveles altos de acercamiento.

Rotar la pantalla

Haga clic y arrastre para rotar el video en vivo. O ingrese directamente el ángulo de rotación en el campo de entrada a la derecha del botón .



Captura de pantalla

Haga clic en para capturar una imagen del video en vivo. La imagen capturada se guarda en el formato `capture_{ch1|ch2}_{main|sub}_{YYYY-MM-DDTHH-MM-SS}.jpeg`.



Modo de pantalla completa

Use el modo de pantalla completa para ver el video en un tamaño mayor. Haga clic en en la esquina inferior derecha de la pantalla.



- Los cambios de modo de visualización y el acercamiento siguen disponibles en el modo de pantalla completa.
- Para salir del modo de pantalla completa, presione la tecla ESC o haga clic de nuevo en .

Opciones de visualización de IA

Haga clic en en la esquina superior derecha de la pantalla para establecer las opciones de visualización de IA del video en vivo.



- **Event Box Popup**: Cuando ocurre un evento de IA, el evento aparece como una ventana emergente en la esquina superior izquierda del video en vivo.
- **User Box Popup**: Cuando una cara se detecta mediante un evento de IA, el cuadro de usuario aparece como una ventana emergente en la esquina inferior derecha del video en vivo.
- **Default Opacity**: Ajuste la opacidad de las ventanas emergentes de eventos y de usuarios.
- **Reference Point**: Muestre un punto de referencia sobre el cuadro de detección de personas en el video en vivo. Habilite esta opción para mostrar una leyenda en la esquina superior derecha del video.
  - Punto azul claro (🔵): Centro del cuadro.
  - Punto rojo (🔴): 80% desde la parte superior a lo largo del eje longitudinal del cuadro. Si instala la cámara en el techo apuntando hacia abajo, el punto aparece cerca de los pies de la persona.

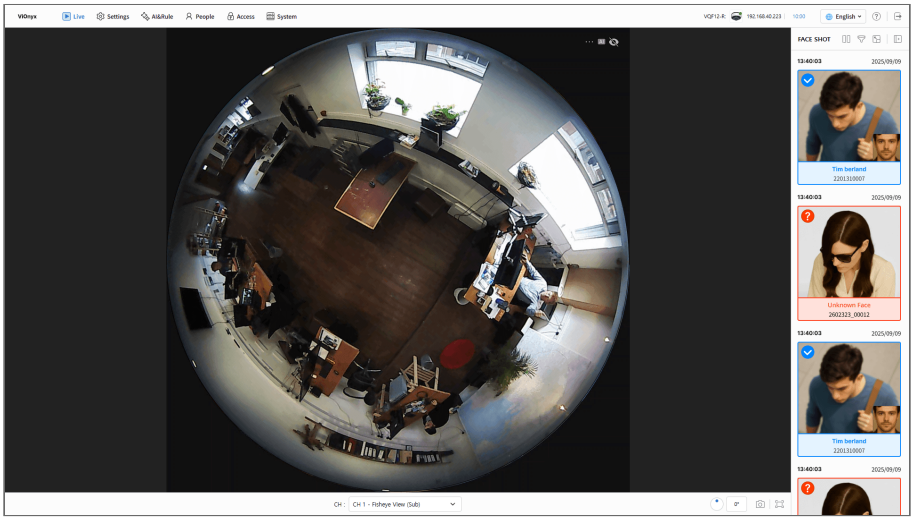
Información

- La ventana emergente permanece visible durante el tiempo configurado en la opción **Display Time** (en segundos).
- Use la opción **Reference Point** solo cuando la característica de IA (AI 👁) esté habilitada.
- La versión de firmware 1.1.0 o posterior incluye soporte para las opciones **Default Opacity** y **Reference Point**.

Abra el panel Face Shot

Si habilitó la función de eventos de IA, puede revisar las caras detectadas por la cámara. Para abrir el panel **Face Shot**, haga

clic en en la esquina superior derecha de la pantalla.



Haga clic en los iconos de herramientas en la parte superior del panel **Face Shot** para usar estas funciones:

- / : Pausar o reanudar Face Shot.
- : Filtrar los resultados de Face Shot.
- : Expandir el panel **Face Shot** a pantalla completa.

> **Información**
> Para obtener más información sobre las opciones de eventos de IA y reglas, consulte Administrar Eventos de IA.

Cuando el video no se reproduce

Si el video de la cámara no carga, siga estos pasos para comprobar la conexión de red.

1. Verifique las conexiones de la cámara y de red.
2. Presione **Actualizar (F5)** en su navegador web.
3. El sistema intenta reconectarse automáticamente.

Administrar Eventos de IA

Definir eventos y reglas de IA permite que la cámara ejecute automáticamente las acciones requeridas ante situaciones detectadas. Cree un evento de IA para cada situación y luego vincule la acción del evento a una regla de IA.

Cree eventos de IA para objetivos de vigilancia como movimiento, intrusión en zonas, cruce de línea, conteo de personas y aproximación a la puerta. En las reglas de IA, especifique acciones de audio, webhook y relé y aplique horarios para limitar cuándo se ejecutan las acciones. Ajuste las opciones de autenticación facial en los ajustes avanzados según su entorno.

> **Información**
> Para usar eventos de IA, configure al menos un área facial que se aplique a todos los eventos.

Configurar Eventos de Seguimiento de Personas

Crea eventos de seguimiento de personas para detectar la entrada en áreas restringidas. Agrega áreas de rostro de forma opcional para priorizar el seguimiento facial en zonas específicas; los usuarios registrados se identifican automáticamente.

¿Cuándo usarlo?

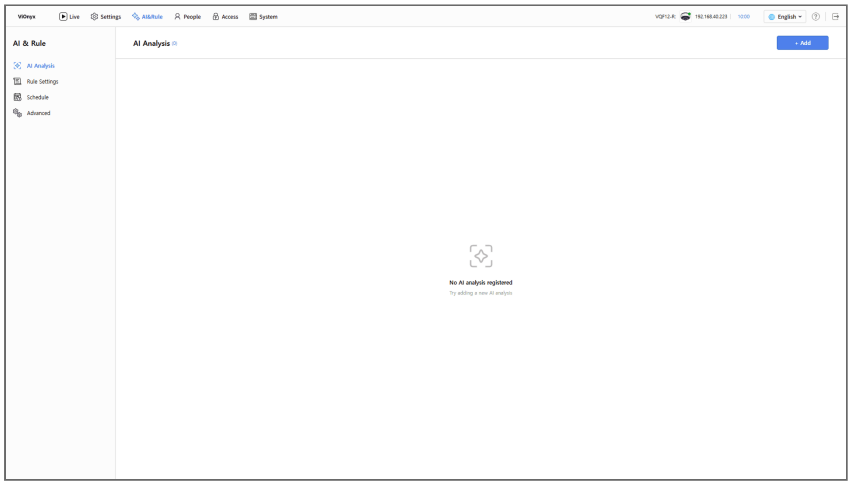
- Supervisa la entrada y la salida de empleados o clientes registrados en el área de entrada.
- Supervisa el acceso a áreas seguras (salas de reuniones, almacenamiento).
- Sigue el flujo de clientes hacia rincones específicos de la tienda (nuevos productos, zonas de eventos).

Crear eventos de seguimiento de personas

Cree eventos de seguimiento de usuarios para seguir el movimiento de las personas en tiempo real en Vista en vivo. Además, definir áreas de rostro reconoce a los usuarios registrados e identifica quién se movió.

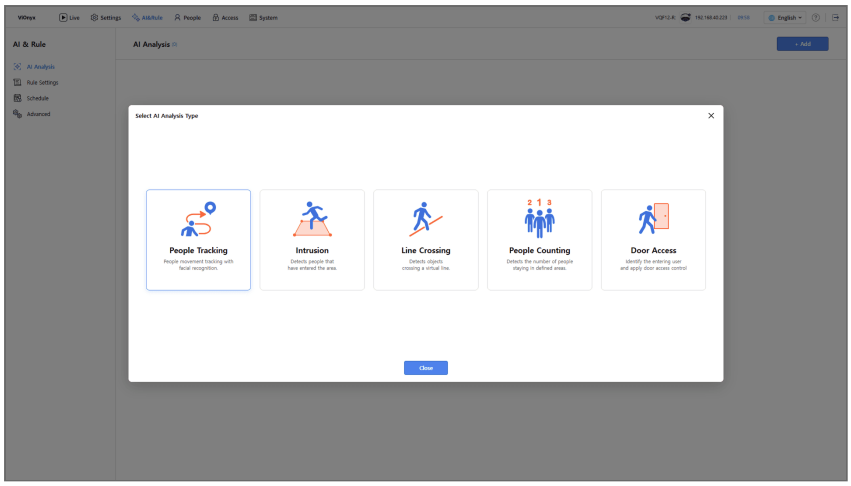
1 Iniciar creación del evento

1. Haga clic en el menú **AI&Rule** en la esquina superior izquierda de la pantalla.
2. Haga clic en **AI Analysis** en la barra lateral izquierda.

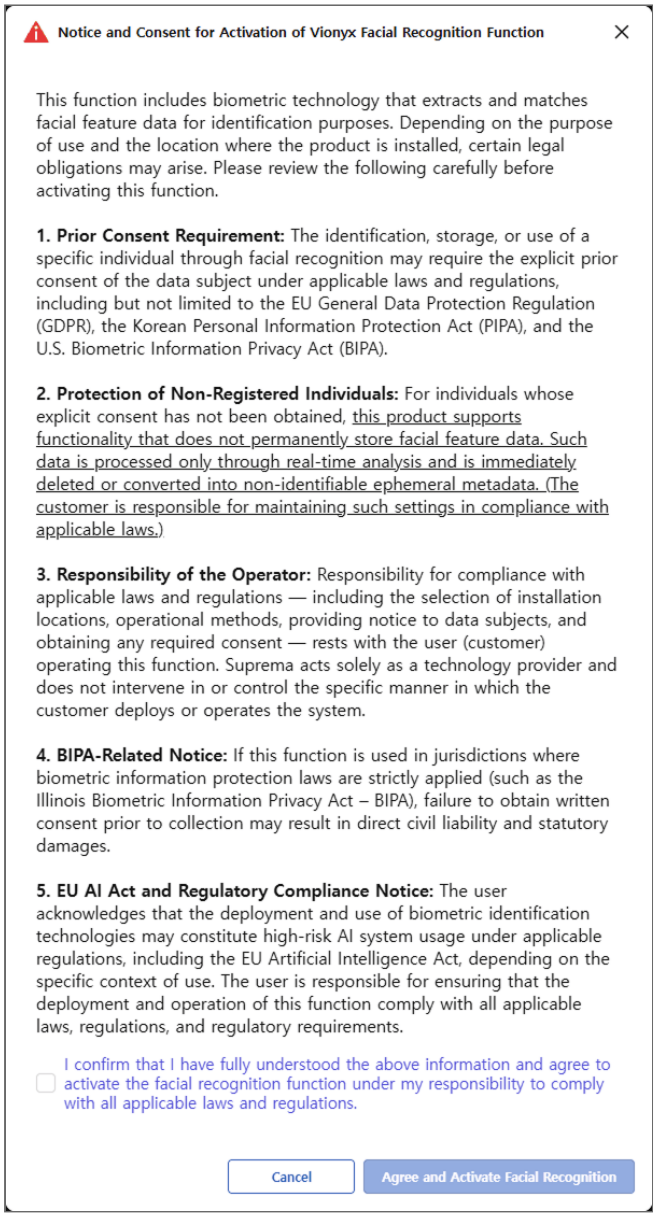


3. Haga clic en **+ Add** en la esquina superior derecha de la pantalla.

4. Haz clic en **People Tracking** en la ventana **Select AI Analysis Type**.

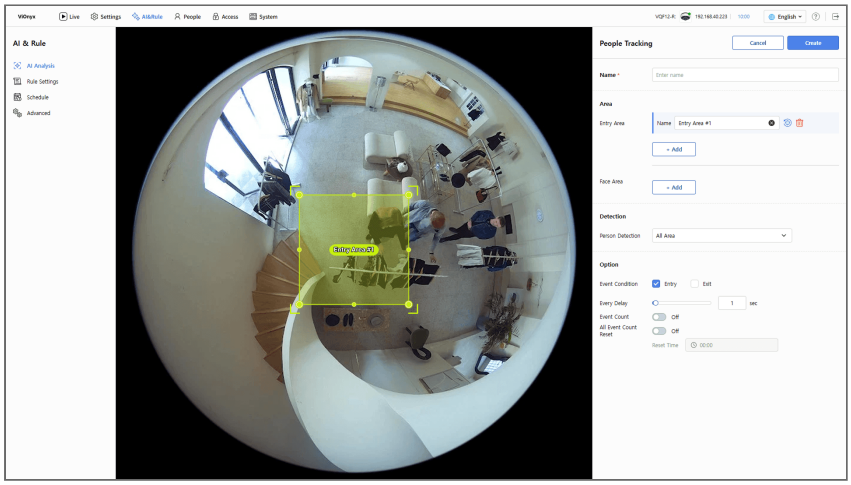


5. Cuando aparece la ventana emergente **Notice and Consent for Activation of Vionyx Facial Recognition Function**, revise los detalles, seleccione la casilla de consentimiento y haga clic en **Agree and Activate Facial Recognition**.



- Para usar la función de Facial Authentication, cumpla con las normas locales. No puede continuar sin consentimiento.
- La ventana emergente **Notice and Consent for Activation of Vionyx Facial Recognition Function** aparece solo una vez. La creación posterior de eventos de IA asume el consentimiento.

6. Completa la configuración necesaria en el panel derecho **People Tracking**.

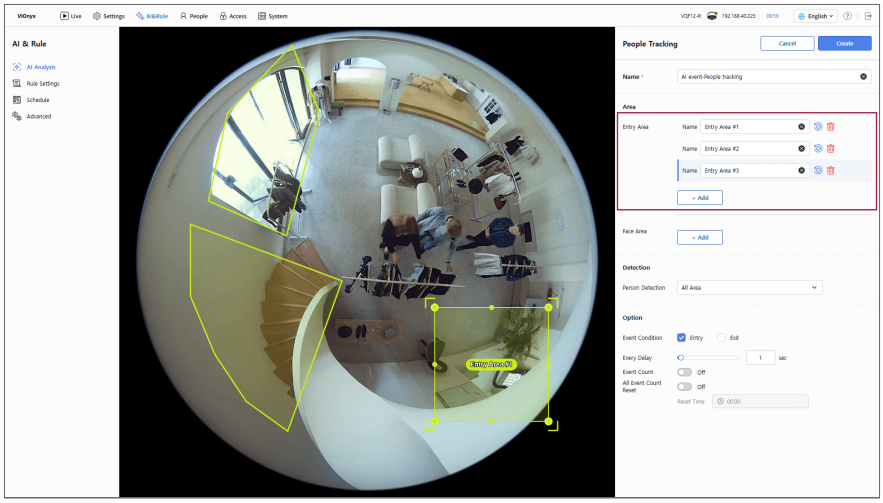


2 Configurar nombre del evento

Ingrese el nombre del evento de IA en el campo **Name**. El nombre puede tener hasta 64 caracteres.

3 Configuración del área de entrada

Define el área de entrada que se va a seguir. La cámara detecta entradas y salidas en el área configurada. Configure al menos una línea virtual. Haga clic en **+ Add** para agregar hasta 10. Aparece un recuadro amarillo en la vista en vivo. Arrastra las esquinas o los puntos con el mouse para ajustar la forma. Arrastre el centro para mover la línea.



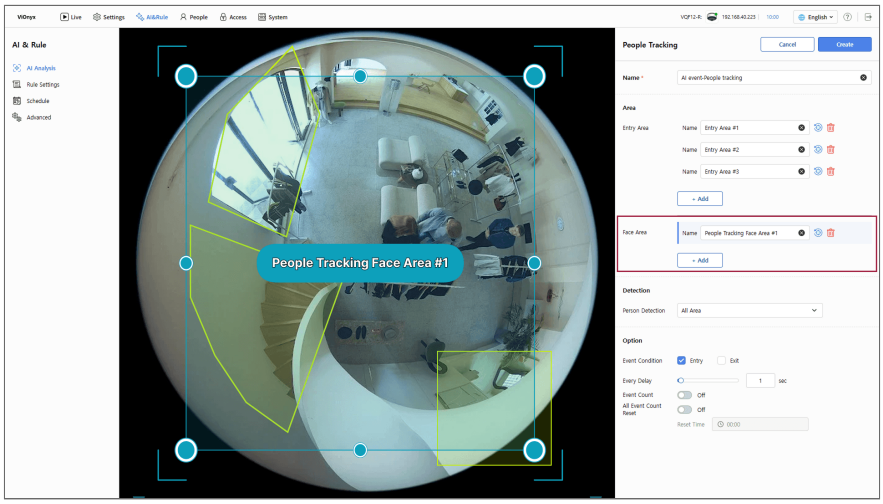
- **Name**: Edita el nombre del área de entrada. Asigne un nombre claro y descriptivo. El nombre del área de entrada aparece al pasar el mouse por encima en la vista en vivo.

Información

- Haz clic en para restablecer la forma y el tamaño del área de entrada configurada.
- Haz clic en para eliminar un área de entrada agregada.

4 Ajustes del área facial (opcional)

Defina el área para la detección facial. Cuando se configura, el sistema prioriza el seguimiento facial en esa área. Configura el área de rostro para incluir el área de entrada. Si el área de rostro no incluye el área de entrada, la cámara no puede reconocer rostros. Haga clic en **+ Add** para agregar hasta 10 áreas faciales. Aparece un cuadro azul en Live View; arrastre las esquinas o los puntos para ajustar la forma. Arrastre el centro para mover la línea.



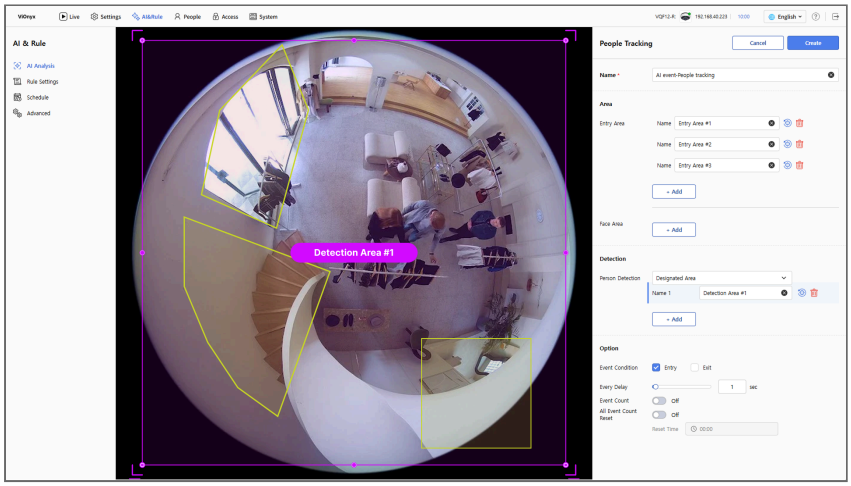
- **Name**: edite el nombre del área facial. Asigne un nombre claro y descriptivo. El nombre del área facial aparece al pasar el cursor en Live View.

> **Información**
>
> - Los usuarios enrolados se identifican automáticamente en el menú **Live** y se muestran por nombre. Los usuarios no enrolados aparecen como **Unknown Face**.
> - Haga clic en para restablecer la forma y el tamaño del área facial configurada.
> - Haga clic en para eliminar un área facial agregada.
> - En los ajustes de la cámara, si usa la opción **Adaptive AE mode**, ajústela. Haga que el área del rostro incluya el lugar donde una persona se coloca o pasa. Verifique que el rostro aparezca con claridad.

5 Ajustes de detección de personas (opcional)

En la sección **Detection**, seleccione el área donde la cámara detecta personas. Reduzca el área de detección según sea necesario para reducir detecciones falsas en áreas irrelevantes (finales de pasillos, ventanas, superficies reflectantes, etc.).

- **All Area**: Predeterminado. Detecta personas en toda la pantalla. Disponible independientemente de si se establecen áreas faciales.
- **Designated Area**: Detecta personas solo dentro del área que especifique. Disponible solo cuando no se establece un área facial. Configure al menos una línea virtual. Haga clic en **+ Add** para agregar hasta 10. Aparece un cuadro morado en la vista en vivo; arrastre sus esquinas o puntos con el mouse para ajustarlo a la forma deseada. Arrastre el centro para mover la línea.



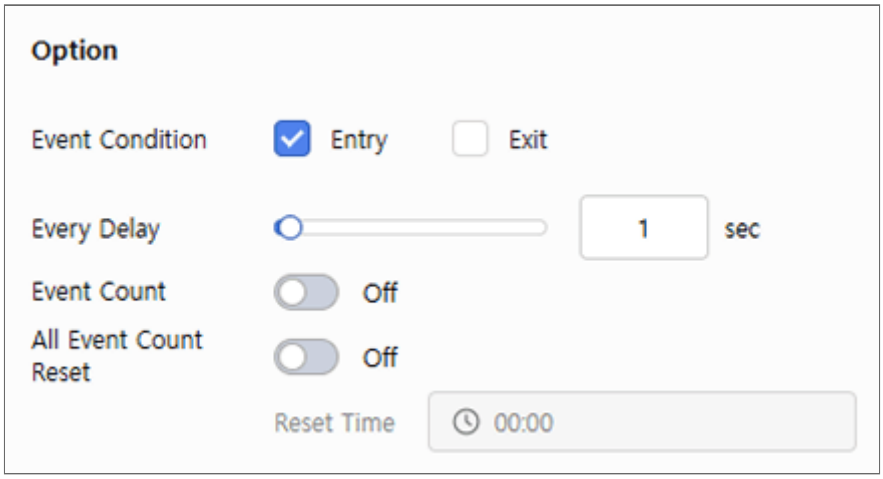
– **Name**: Edite el nombre del área de detección de personas.

- **Face Area Only**: Detecta personas solo dentro del área facial. Disponible solo cuando se establece un área facial.

> **Información**
>
> - Al agregar un área facial con **Designated Area** seleccionado, el sistema abre la ventana emergente **Notice**. Haga clic en **OK** para borrar el área de detección designada y cambiar a **Face Area Only**.
> - Al eliminar todas las áreas faciales con **Face Area Only** seleccionado, el sistema cambia automáticamente a **All Area**.
> - En los ajustes de la cámara, al usar la opción **Adaptive AE mode**, limite el rango a **Designated Area** o **Face Area Only**. Mantenga pantallas, fotos o pósteres con rostros fuera del área de detección.
> - Haga clic en para inicializar la forma y el tamaño del área de detección de personas.
> - Haga clic en para eliminar el área de detección de personas agregada.
> - La versión de firmware 1.1.0 o posterior incluye soporte para esta característica.

6 Configurar condiciones de activación de eventos y ajustes de conteo de eventos

En la sección **Option**, configure las condiciones de activación de eventos y el conteo de eventos.



- **Event Condition**: Seleccione la acción que activa un evento. Opcionalmente, seleccione **Entry** y **Exit**.
- **Every Delay**: Establezca la duración mínima para tratarla como un evento. Un evento ocurre solo cuando el estado de detección dura más que el tiempo establecido. Se puede configurar hasta un máximo de 60 segundos.

  > Si ocurren demasiados eventos, aumente el valor de **Every Delay**. El movimiento detectado por menos del tiempo establecido no se considera un evento, lo que reduce eventos innecesarios.

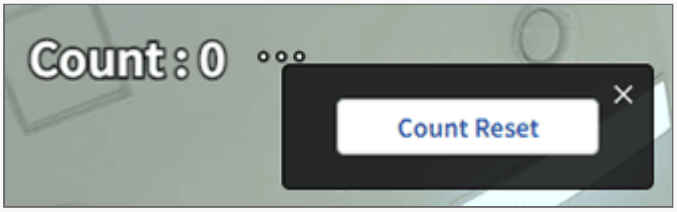
- **Event Count**: Establezca esta opción en **On** para contar cuántas veces las personas entran o salen del área de entrada. El sistema cuenta las entradas y las salidas por separado. Si existen varias áreas de entrada, el sistema cuenta cada área por separado.

  > El sistema cuenta solo las opciones seleccionadas en **Event Condition**. Por ejemplo, si solo se selecciona **Entry**, solo las entradas aparecen como eventos y el sistema las registra en los registros.

- **All Event Count Reset**: Establezca esta opción en **On** para inicializar diariamente los conteos de eventos de todas las áreas de entrada a la hora especificada. El sistema inicializa los conteos de eventos de todas las áreas de entrada a la hora establecida en **Reset Time**.

Información

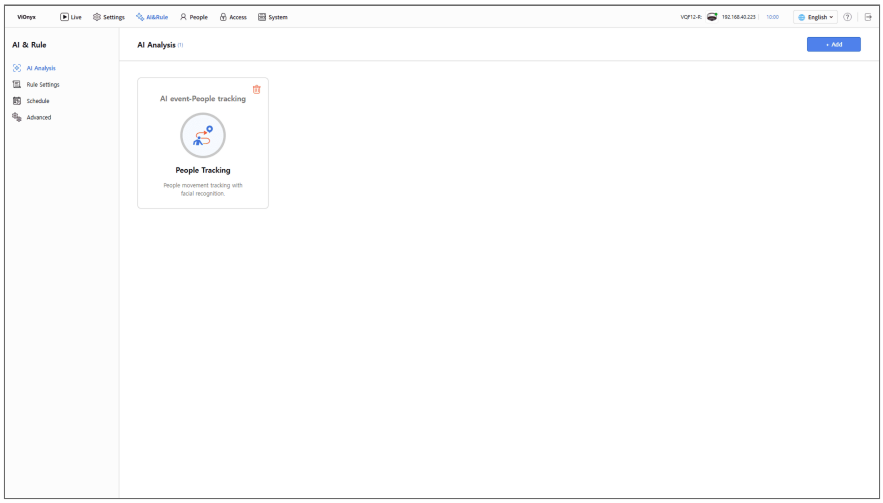
- Si configura **Event Count** en **On**, el menú **Live** muestra **Count : N** para cada área de entrada en el video. Haga clic en el botón ••• y seleccione **Count Reset** para inicializar manualmente el conteo de eventos.



- El firmware versión 1.1.0 o posterior incluye soporte para las opciones de conteo de eventos.

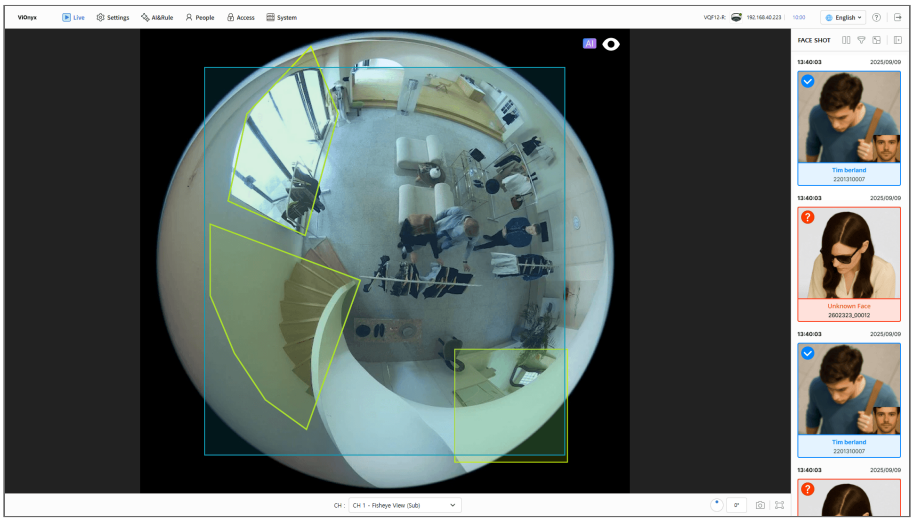
7 Guardar ajustes

Después de completar todas las configuraciones, haga clic en **Create** en la esquina superior derecha. La interfaz vuelve a la pantalla anterior y agrega el nuevo evento de IA a la lista.



Verificar en Live

Haga clic en el menú **Live** en la esquina superior izquierda de la pantalla. Confirme que el ícono AI en la esquina superior derecha de la transmisión de la cámara esté activado. Las áreas de entrada y de rostro configuradas aparecen como superposiciones sobre el video. Se activa un evento cada vez que una persona entra o sale de un área de entrada. Si se configuran áreas faciales, la cámara detecta rostros allí; los usuarios enrolados se identifican automáticamente y sus nombres aparecen.



Información

- Los usuarios no enrolados aparecen como **Unknown Face**. Los usuarios enrolados aparecen con su nombre.
- Si la cámara no logra reconocer rostros, activa la opción **Min Face Size Visualize**. Como alternativa, amplía el área de rostro o ajusta la posición de la cámara.
- La mala iluminación o la luz de fondo pueden impedir que la cámara detecte rostros. Mejore la iluminación del área o ajuste la posición y el ángulo de la cámara para que los rostros se vean con claridad.
- Los rostros deben mirar a la cámara para que la cámara los detecte. Es posible que la cámara no detecte las vistas de perfil o de espaldas.
- Si no se producen eventos en el área de entrada, verifica que el área de rostro la incluya.

Configurar Eventos de Detección de Intrusión

Un evento de detección de intrusión genera un evento en tiempo real cuando una persona entra o sale de un área definida por el administrador. Agregue áreas faciales de forma opcional para priorizar el seguimiento facial dentro de esas zonas; los usuarios inscritos se autentican automáticamente. Reciba alertas en tiempo real cuando personas no autorizadas entren en áreas que requieren monitoreo.

¿Cuándo usarlo?

- Detección de intrusión en tiempo real para personas no autorizadas en áreas que requieren seguridad
- Reciba alertas en tiempo real cuando alguien entre fuera del horario laboral o en un área que requiere monitoreo
- Detecte cuándo personas no inscritas entran en un área de monitoreo
- Registre y haga seguimiento del acceso a áreas de alto riesgo.

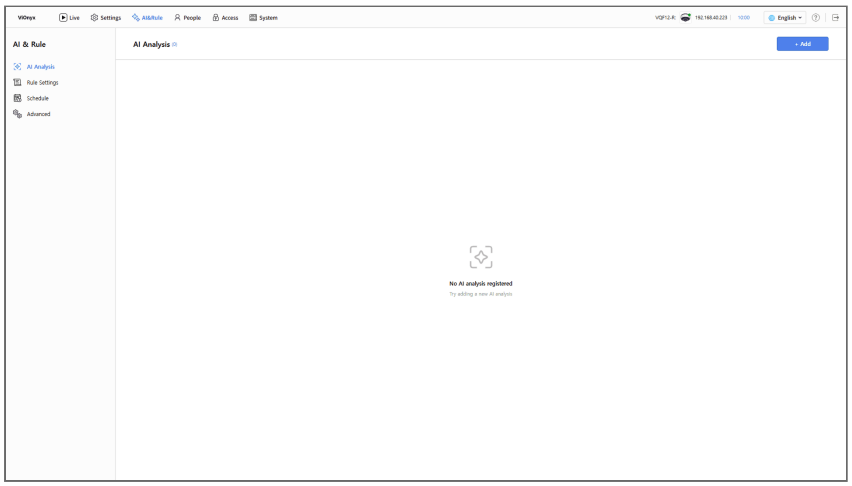
> **Información**
> Use esto para fines distintos del control de acceso, y la cámara no determina si el acceso está restringido.

Crear evento de detección de intrusión

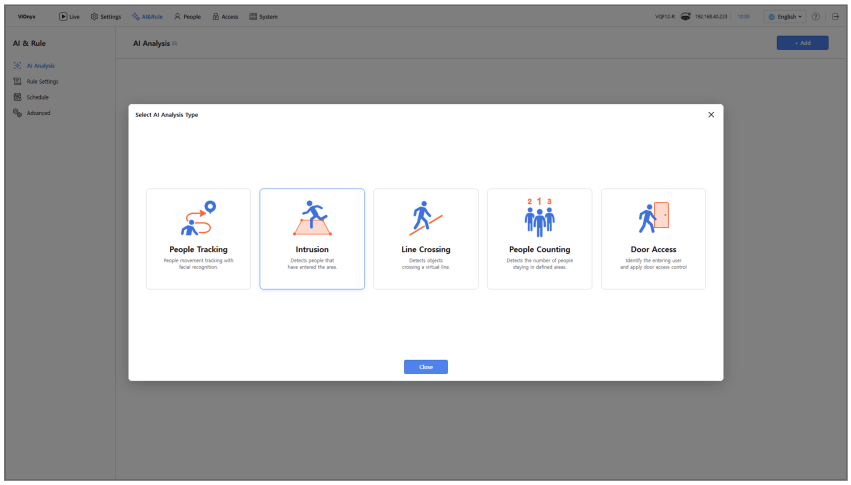
Crear un evento de detección de intrusión permite que el menú **Live** detecte cuándo una persona entra en un área específica y genere eventos. Además, al configurar un área facial, se prioriza el seguimiento facial en esa área; los usuarios enrolados se identifican automáticamente.

1 Iniciar creación del evento

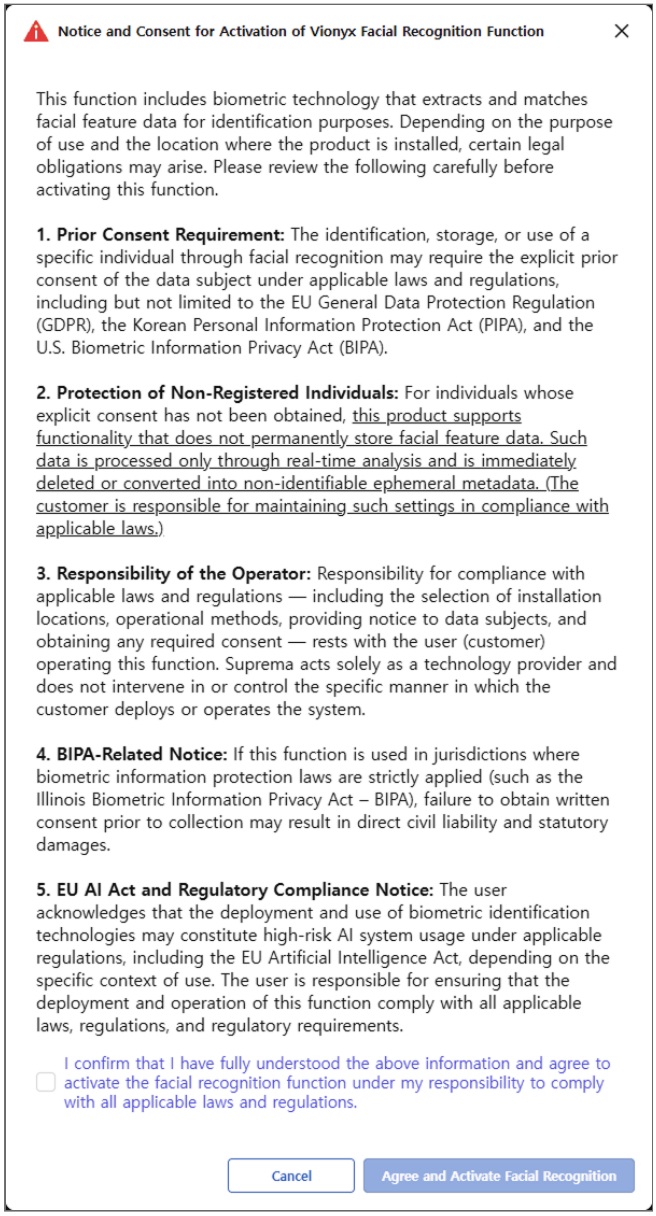
1. Haga clic en el menú **AI&Rule** en la esquina superior izquierda de la pantalla.
2. Haga clic en **AI Analysis** en la barra lateral izquierda.



3. Haga clic en **+ Add** en la esquina superior derecha de la pantalla.
4. Haga clic en **Intrusion** en la ventana **Select AI Analysis Type**.

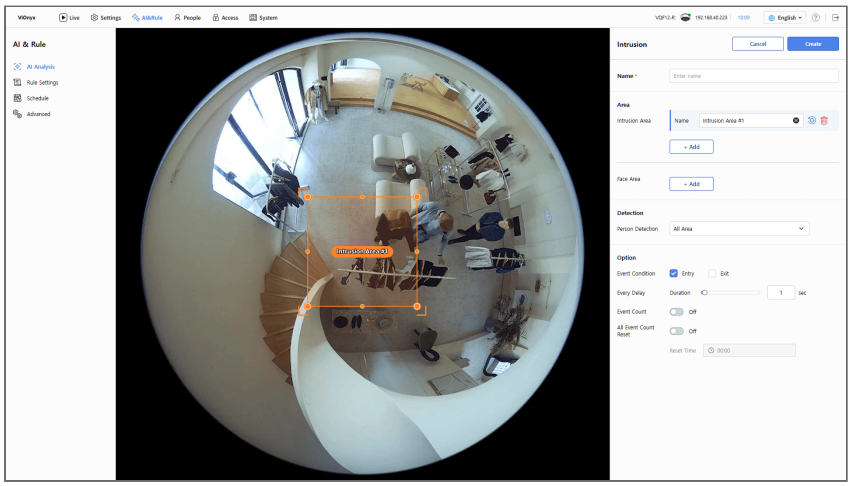


5. Cuando aparece la ventana emergente **Notice and Consent for Activation of Vionyx Facial Recognition Function**, revise los detalles, seleccione la casilla de consentimiento y haga clic en **Agree and Activate Facial Recognition**.



- Para usar la función de Facial Authentication, cumpla con las normas locales. No puede continuar sin consentimiento.
- La ventana emergente **Notice and Consent for Activation of Vionyx Facial Recognition Function** aparece solo una vez. La creación posterior de eventos de IA asume el consentimiento.

6. Complete los ajustes requeridos en el panel **Intrusion** de la derecha.

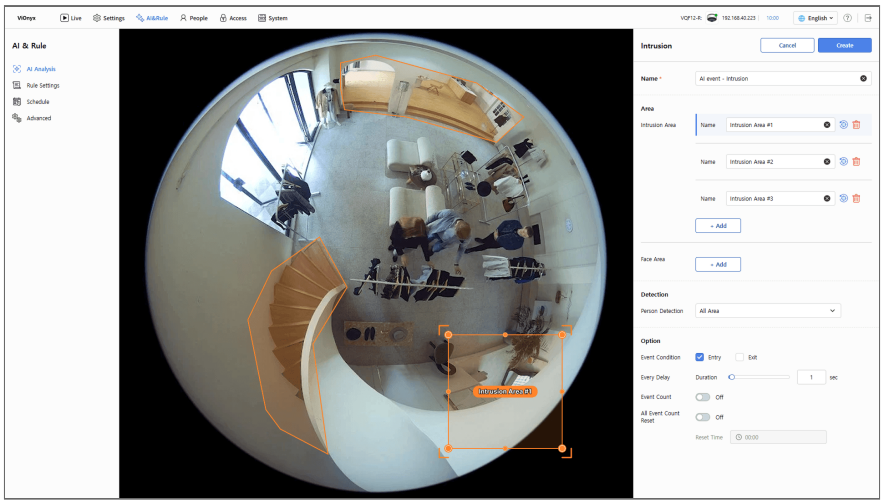


2 Configurar nombre del evento

Ingrese el nombre del evento de IA en el campo **Name**. El nombre puede tener hasta 64 caracteres.

3 Ajustes del área de intrusión

Configure el área de intrusión. La cámara detecta entradas y salidas en el área configurada. Configure al menos una línea virtual. Haga clic en **+ Add** para agregar hasta 10. Aparece un cuadro naranja en la vista en vivo; arrastre sus esquinas o puntos con el mouse para ajustarlo a la forma deseada. Arrastre el centro para mover la línea.



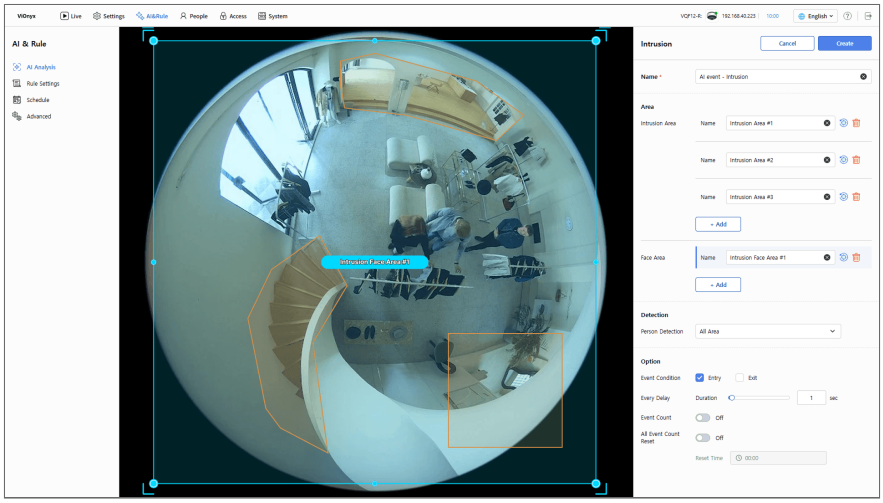
- **Name**: Edite el nombre del área de intrusión. Asigne un nombre claro y descriptivo. El nombre del área de intrusión aparece al pasar el mouse por encima en la vista en vivo.

Información

- Para inicializar la forma y el tamaño de un área de intrusión configurada, haga clic en .
- Para eliminar un área de intrusión agregada, haga clic en .

4 Ajustes del área facial (opcional)

Defina el área para la detección facial. Cuando se configura, el sistema prioriza el seguimiento facial en esa área. Clasifique a las personas detectadas en áreas faciales como usuarios autenticados o personas no autorizadas para identificar con claridad a los entrantes autorizados y a los intrusos. Las áreas faciales y las áreas de intrusión pueden superponerse. Haga clic en **+ Add** para agregar hasta 10 áreas faciales. Aparece un cuadro azul en Live View; arrastre las esquinas o los puntos para ajustar la forma. Arrastre el centro para mover la línea.



- **Name**: edite el nombre del área facial. Asigne un nombre claro y descriptivo. El nombre del área facial aparece al pasar el cursor en Live View.

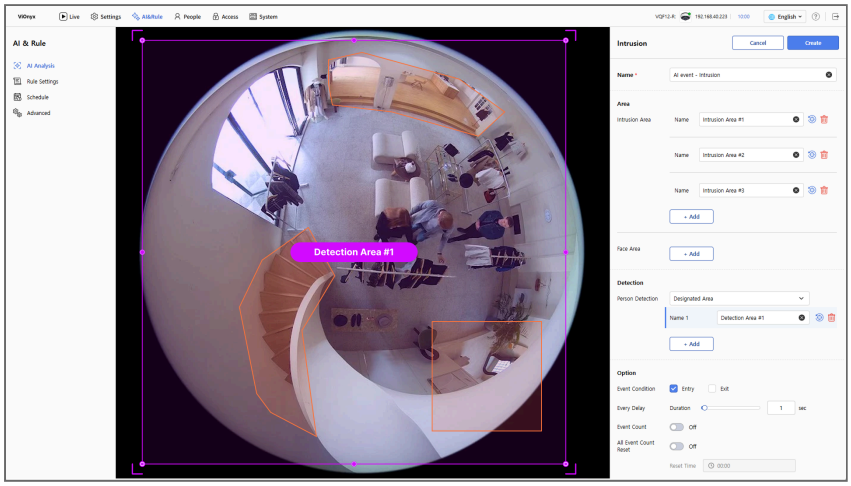
Información

- Los usuarios enrolados se identifican automáticamente en el menú **Live** y se muestran por nombre. Los usuarios no enrolados aparecen como **Unknown Face**.
- Haga clic en para restablecer la forma y el tamaño del área facial configurada.
- Haga clic en para eliminar un área facial agregada.
- En los ajustes de la cámara, si usa la opción **Adaptive AE mode**, ajústela. Haga que el área del rostro incluya el lugar donde una persona se coloca o pasa. Verifique que el rostro aparezca con claridad.

5 Ajustes de detección de personas (opcional)

En la sección **Detection**, seleccione el área donde la cámara detecta personas. Reduzca el área de detección según sea necesario para reducir detecciones falsas en áreas irrelevantes (finales de pasillos, ventanas, superficies reflectantes, etc.).

- **All Area**: Predeterminado. Detecta personas en toda la pantalla. Disponible independientemente de si se establecen áreas faciales.
- **Designated Area**: Detecta personas solo dentro del área que especifique. Disponible solo cuando no se establece un área facial. Configure al menos una línea virtual. Haga clic en **+ Add** para agregar hasta 10. Aparece un cuadro morado en la vista en vivo; arrastre sus esquinas o puntos con el mouse para ajustarlo a la forma deseada. Arrastre el centro para mover la línea.



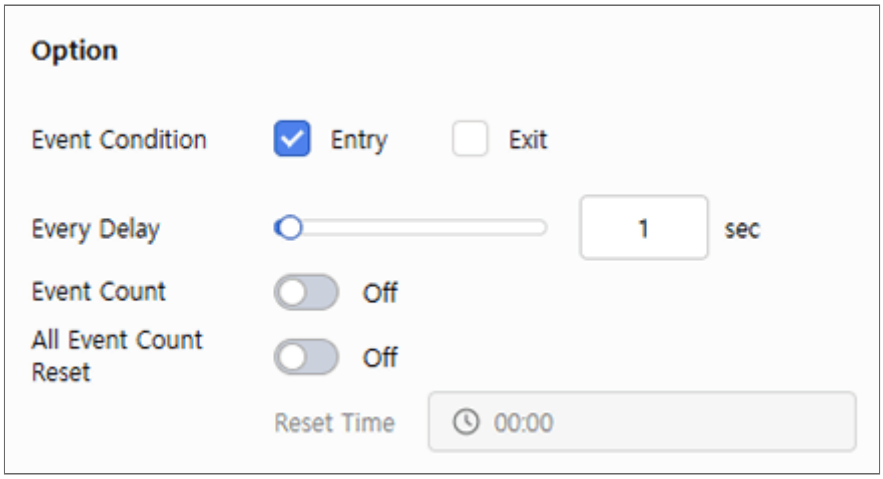
  - **Name**: Edite el nombre del área de detección de personas.
- **Face Area Only**: Detecta personas solo dentro del área facial. Disponible solo cuando se establece un área facial.

Información

- Al agregar un área facial con **Designated Area** seleccionado, el sistema abre la ventana emergente **Notice**. Haga clic en **OK** para borrar el área de detección designada y cambiar a **Face Area Only**.
- Al eliminar todas las áreas faciales con **Face Area Only** seleccionado, el sistema cambia automáticamente a **All Area**.
- En los ajustes de la cámara, al usar la opción **Adaptive AE mode**, limite el rango a **Designated Area** o **Face Area Only**. Mantenga pantallas, fotos o pósteres con rostros fuera del área de detección.
- Haga clic en para inicializar la forma y el tamaño del área de detección de personas.
- Haga clic en para eliminar el área de detección de personas agregada.
- La versión de firmware 1.1.0 o posterior incluye soporte para esta característica.

6 Configurar condiciones de activación de eventos y ajustes de conteo de eventos

En la sección **Option**, configure las condiciones de activación de eventos y el conteo de eventos.



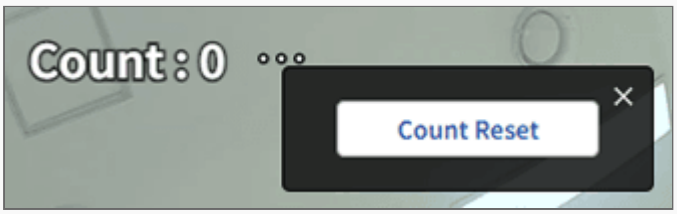
- **Event Condition**: Seleccione la acción que activa un evento. Opcionalmente, seleccione **Entry** y **Exit**.
- **Every Delay**: Establezca la duración mínima para tratarla como un evento. Un evento ocurre solo cuando el estado de detección dura más que el tiempo establecido. Se puede configurar hasta un máximo de 60 segundos.

  > Si ocurren demasiados eventos, aumente el valor de **Every Delay**. El movimiento detectado por menos del tiempo establecido no se considera un evento, lo que reduce eventos innecesarios.

- **Event Count**: Configúrelo en **On** para contar entradas y salidas en un área de intrusión. El sistema cuenta por separado las entradas y salidas de cada área de intrusión.

  > El sistema cuenta solo las opciones seleccionadas en **Event Condition**. Por ejemplo, si solo se selecciona **Entry**, solo las entradas aparecen como eventos y el sistema las registra en los registros.

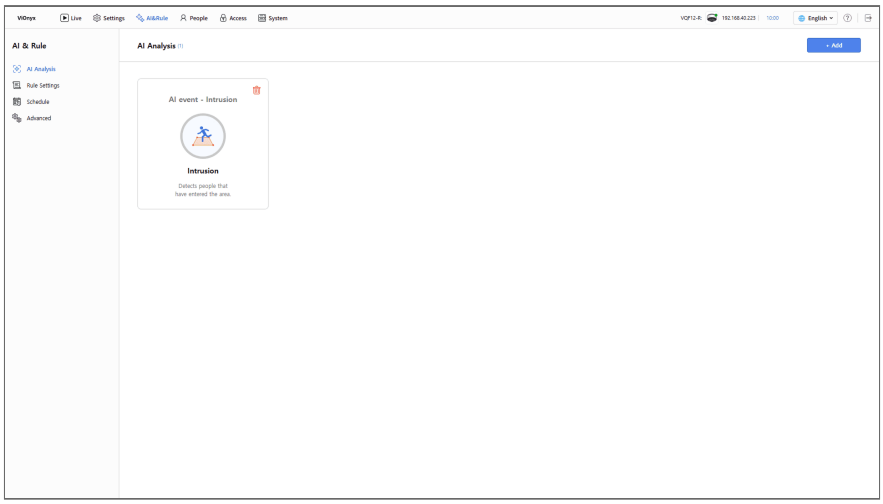
- **All Event Count Reset**: Configúrelo en **On** para inicializar a diario los conteos de eventos de todas las áreas de intrusión a la hora especificada. El sistema inicializa los conteos de eventos de todas las áreas de intrusión a la hora definida en **Reset Time**.

> **Información**
>
> - Si **Event Count** está en **On**, en el menú **Live** aparece **Count : N** sobre el video para cada área de intrusión. Haga clic en el botón ••• y seleccione **Count Reset** para inicializar manualmente el conteo de eventos.
>
> 
>
>
> - El firmware versión 1.1.0 o posterior incluye soporte para las opciones de conteo de eventos.

7 Guardar ajustes

Después de completar todas las configuraciones, haga clic en **Create** en la esquina superior derecha. La interfaz vuelve

a la pantalla anterior y agrega el nuevo evento de IA a la lista.



Verificar en Live

Haga clic en el menú **Live** en la esquina superior izquierda de la pantalla. Confirme que el ícono AI en la esquina superior derecha de la transmisión de la cámara esté activado. Las áreas de intrusión y las áreas faciales configuradas se superponen sobre el video. Se produce un evento cada vez que una persona entra o sale de un área de intrusión. Si configura áreas faciales, la cámara detecta rostros allí; identifica automáticamente a los usuarios enrolados y muestra sus nombres.



Información

- Los usuarios no enrolados aparecen como **Unknown Face**. Los usuarios enrolados aparecen con su nombre.
- La mala iluminación o la luz de fondo pueden impedir que la cámara detecte rostros. Mejore la iluminación del área o ajuste la posición y el ángulo de la cámara para que los rostros se vean con claridad.
- Los rostros deben mirar a la cámara para que la cámara los detecte. Es posible que la cámara no detecte las vistas de perfil o de espaldas.

Configurar Evento de Detección de Cruce de Línea

Configurar un evento de detección de cruce de línea detecta a las personas que cruzan líneas virtuales configuradas y activa eventos en tiempo real. Especifique la dirección de cruce (A→B, B→A o ambas) para supervisar solo una dirección. Agregue opcionalmente un área facial para priorizar el seguimiento de rostros; los usuarios inscritos se identifican automáticamente.

¿Cuándo usarlo?

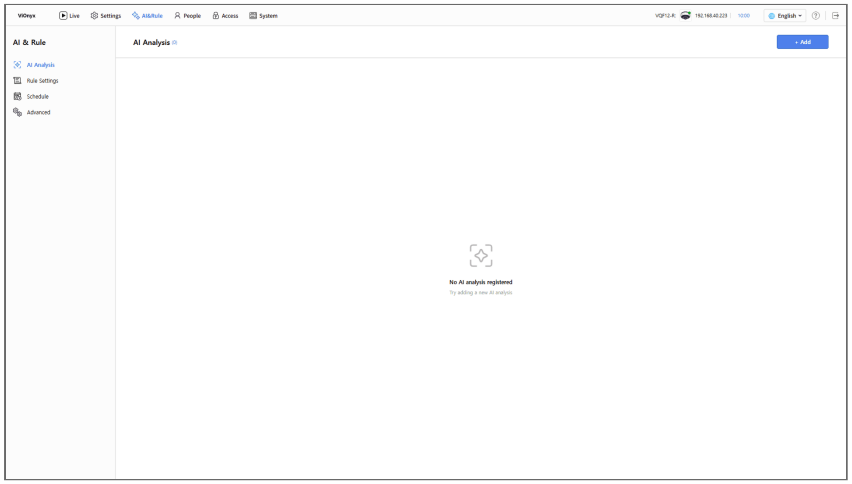
- Supervisar y contar el tráfico en la puerta
- Supervise la entrada solo en una dirección específica (detecta tráfico de un solo sentido)
- Detecte la entrada a áreas específicas fuera del horario laboral
- Rastree el movimiento a la izquierda o derecha del área con respecto a la línea

Crear evento de detección de cruce de línea

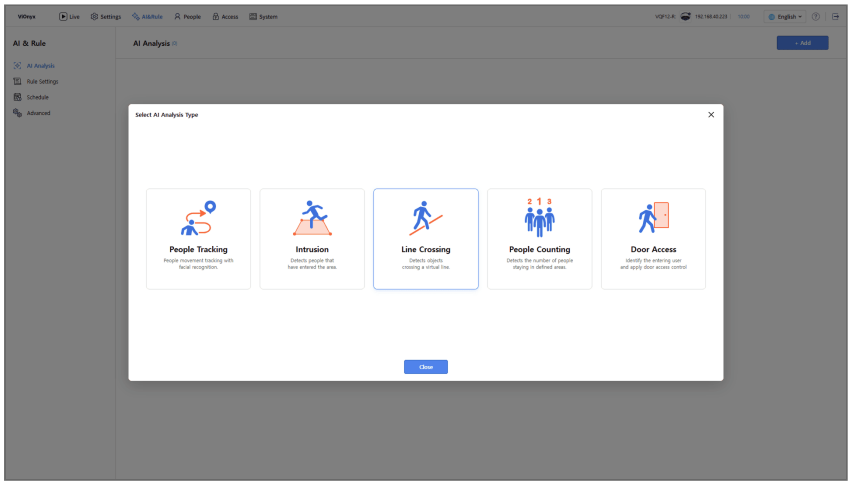
Use el menú **Live** para detectar a las personas que cruzan una línea configurada en un área específica y activar eventos. Además, al configurar un área facial, se prioriza el seguimiento facial en esa área; los usuarios enrolados se identifican automáticamente.

1 Iniciar creación del evento

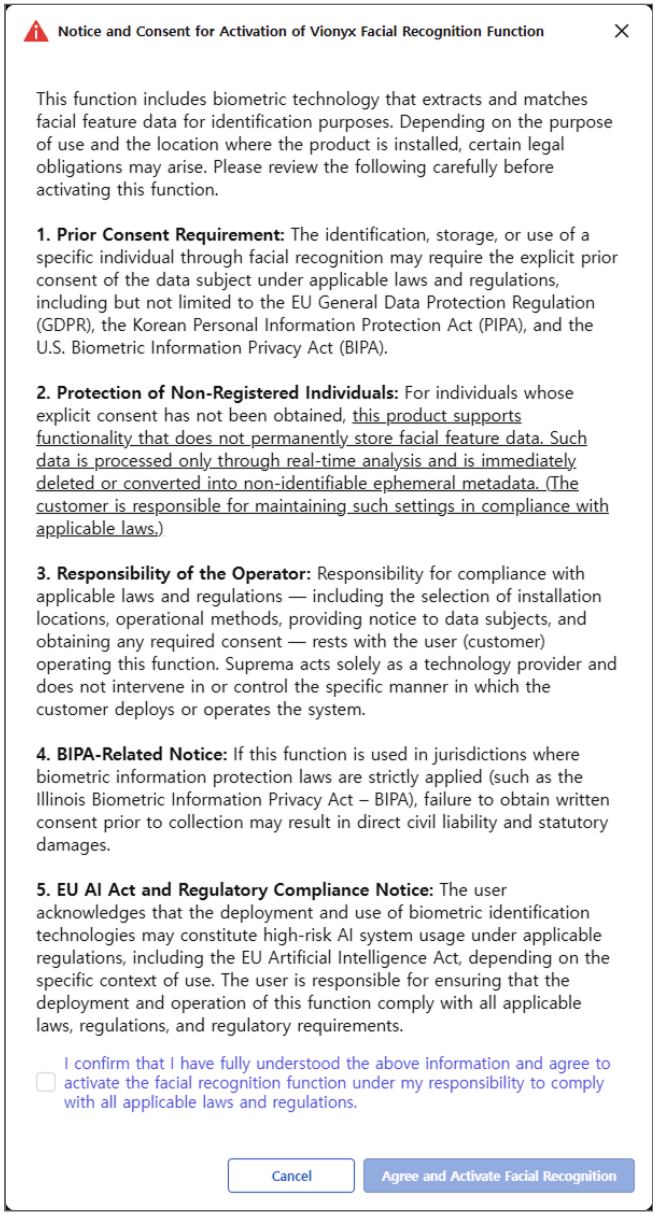
1. Haga clic en el menú **AI&Rule** en la esquina superior izquierda de la pantalla.
2. Haga clic en **AI Analysis** en la barra lateral izquierda.



3. Haga clic en **+ Add** en la esquina superior derecha de la pantalla.
4. En la ventana **Select AI Analysis Type**, haga clic en **Line Crossing**.

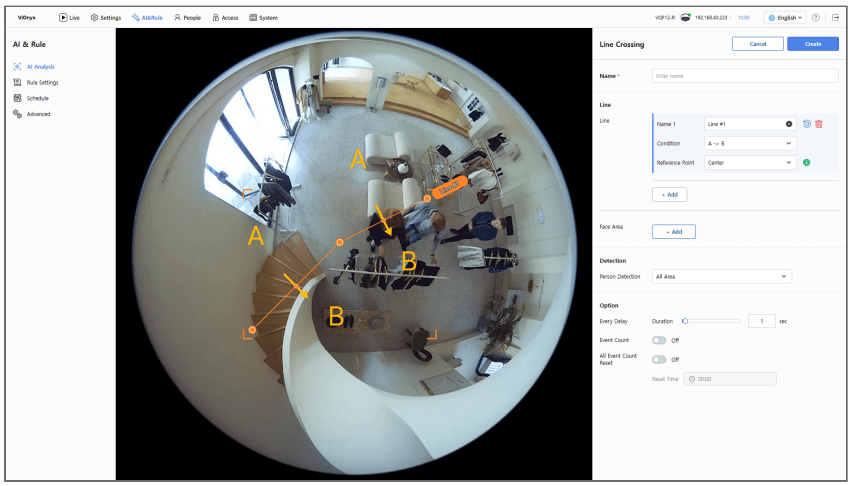


5. Cuando aparece la ventana emergente **Notice and Consent for Activation of Vionyx Facial Recognition Function**, revise los detalles, seleccione la casilla de consentimiento y haga clic en **Agree and Activate Facial Recognition**.



- Para usar la función de Facial Authentication, cumpla con las normas locales. No puede continuar sin consentimiento.
- La ventana emergente **Notice and Consent for Activation of Vionyx Facial Recognition Function** aparece solo una vez. La creación posterior de eventos de IA asume el consentimiento.

6. Complete las configuraciones requeridas en el panel derecho de **Line Crossing**.

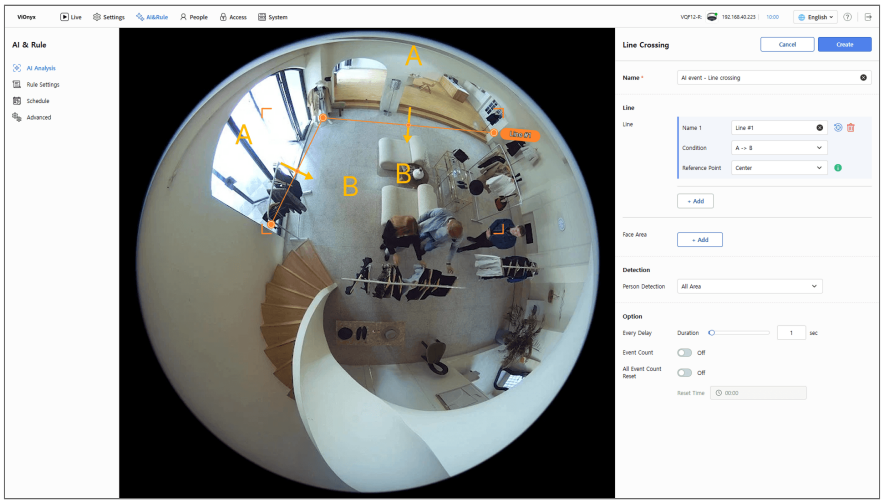


2 Configurar nombre del evento

Ingrese el nombre del evento de IA en el campo **Name**. El nombre puede tener hasta 64 caracteres.

3 Configuración de línea virtual

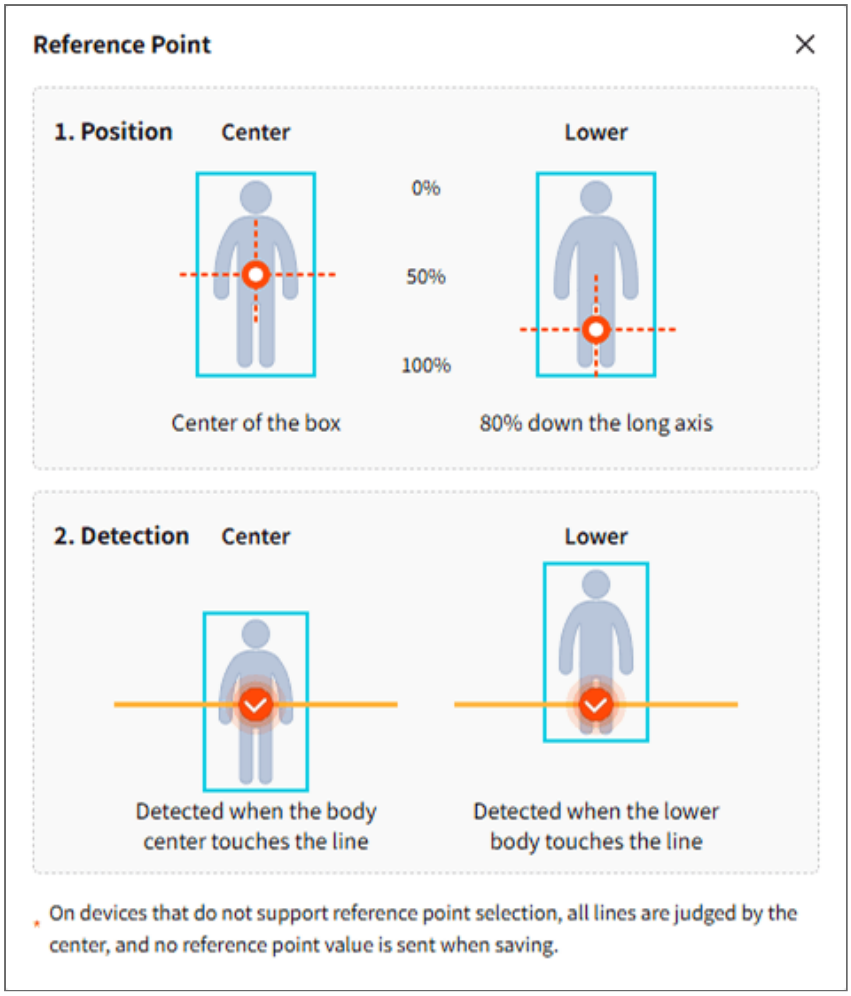
Coloque la línea virtual en la ubicación adecuada en Live View. La cámara detecta a las personas que cruzan líneas virtuales configuradas y activa eventos. Configure al menos una línea virtual. Haga clic en **+ Add** para agregar hasta 10. Aparece una línea naranja en Live View; arrastre las esquinas o los puntos para ajustar la forma. Arrastre el centro para mover la línea.



- **Name**: Edite el nombre de la línea virtual. Asigne un nombre claro y descriptivo. El nombre de la línea virtual aparece al pasar el cursor en Live View.

- **Condition**: Establezca la condición de cruce para la línea virtual. Seleccione una de las tres opciones de dirección a continuación.
  - **A -> B**: Active un evento cuando se cruce de A a B.
  - **B -> A**: Active un evento cuando se cruce de B a A.
  - **A <-> B**: Active un evento cuando se cruce en ambas direcciones.
- **Reference Point**: Seleccione el punto de referencia en el recuadro de detección de personas para determinar si una persona cruza una línea virtual. Establezca esto para cada línea. El valor predeterminado es **Center**.
  - **Center**: Use el centro del recuadro como punto de referencia. El sistema cuenta un cruce cuando el centro del cuerpo toca la línea.
  - **Lower**: Use el punto ubicado al 80 % desde la parte superior a lo largo del eje largo del recuadro. El sistema cuenta un cruce cuando la parte inferior del cuerpo toca la línea. Seleccione esta opción para activar un evento cuando los pies crucen la línea, como si estuviera en el piso.

Haga clic en el icono a la derecha de **Reference Point** para ver la ubicación y los criterios de detección de cada punto de referencia en un diagrama.

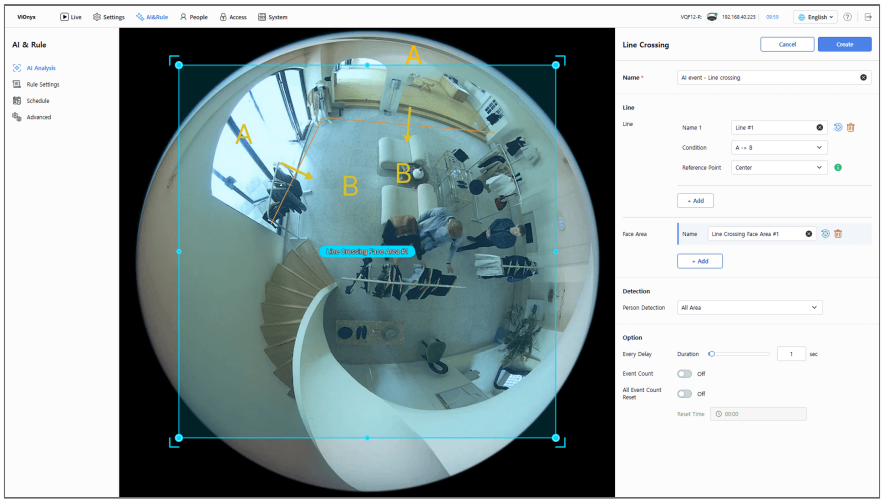


Información

- Se incluye soporte para la opción **Reference Point** en el firmware 1.1.0 o posterior. En dispositivos que no admiten la selección del punto de referencia, todos los cruces de línea usan **Center**.
- **Lower** es una posición calculada a partir del recuadro de detección de personas, no la posición real del pie.
- Active **Reference Point** en Opciones de visualización de IA para ver el punto de referencia en el menú **Live**.
- Haga clic en para restablecer la forma y el tamaño de la línea virtual configurada.
- Haga clic en para eliminar una línea virtual agregada.

4 Ajustes del área facial (opcional)

Defina el área para la detección facial. Cuando se configura, el sistema prioriza el seguimiento facial en esa área. Las áreas faciales pueden superponerse con líneas virtuales. Haga clic en **+ Add** para agregar hasta 10 áreas faciales. Aparece un cuadro azul en Live View; arrastre las esquinas o los puntos para ajustar la forma. Arrastre el centro para mover la línea.



- **Name**: edite el nombre del área facial. Asigne un nombre claro y descriptivo. El nombre del área facial aparece al pasar el cursor en Live View.

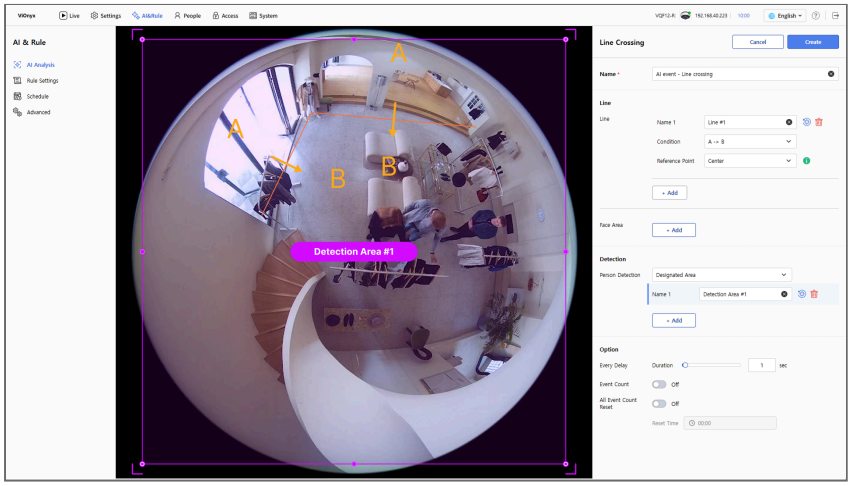
Información

- Los usuarios enrolados se identifican automáticamente en el menú **Live** y se muestran por nombre. Los usuarios no enrolados aparecen como **Unknown Face**.
- Haga clic en para restablecer la forma y el tamaño del área facial configurada.
- Haga clic en para eliminar un área facial agregada.
- En los ajustes de la cámara, si usa la opción **Adaptive AE mode**, ajústela. Haga que el área del rostro incluya el lugar donde una persona se coloca o pasa. Verifique que el rostro aparezca con claridad.

5 Ajustes de detección de personas (opcional)

En la sección **Detection**, seleccione el área donde la cámara detecta personas. Reduzca el área de detección según sea necesario para reducir detecciones falsas en áreas irrelevantes (finales de pasillos, ventanas, superficies reflectantes, etc.).

- **All Area**: Predeterminado. Detecta personas en toda la pantalla. Disponible independientemente de si se establecen áreas faciales.
- **Designated Area**: Detecta personas solo dentro del área que especifique. Disponible solo cuando no se establece un área facial. Configure al menos una línea virtual. Haga clic en **+ Add** para agregar hasta 10. Aparece un cuadro morado en la vista en vivo; arrastre sus esquinas o puntos con el mouse para ajustarlo a la forma deseada. Arrastre el centro para mover la línea.



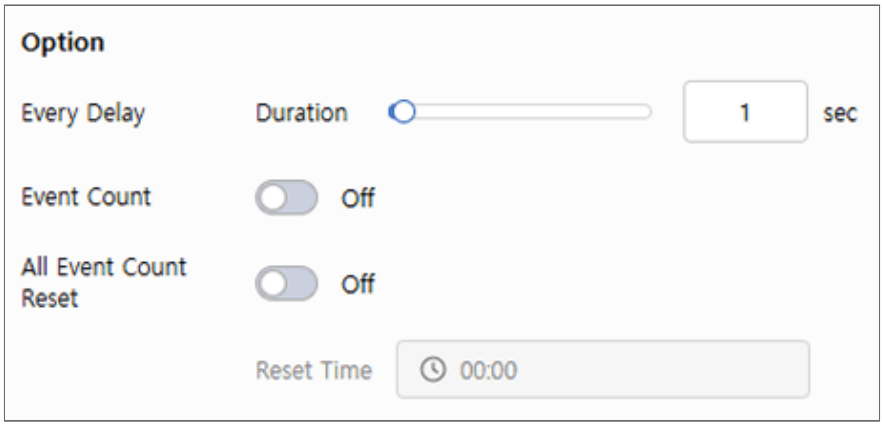
  - **Name**: Edite el nombre del área de detección de personas.
- **Face Area Only**: Detecta personas solo dentro del área facial. Disponible solo cuando se establece un área facial.

Información

- Al agregar un área facial con **Designated Area** seleccionado, el sistema abre la ventana emergente **Notice**. Haga clic en **OK** para borrar el área de detección designada y cambiar a **Face Area Only**.
- Al eliminar todas las áreas faciales con **Face Area Only** seleccionado, el sistema cambia automáticamente a **All Area**.
- En los ajustes de la cámara, al usar la opción **Adaptive AE mode**, limite el rango a **Designated Area** o **Face Area Only**. Mantenga pantallas, fotos o pósteres con rostros fuera del área de detección.
- Haga clic en para inicializar la forma y el tamaño del área de detección de personas.
- Haga clic en para eliminar el área de detección de personas agregada.
- La versión de firmware 1.1.0 o posterior incluye soporte para esta característica.

6 Configurar condiciones de activación de eventos y ajustes de conteo de eventos

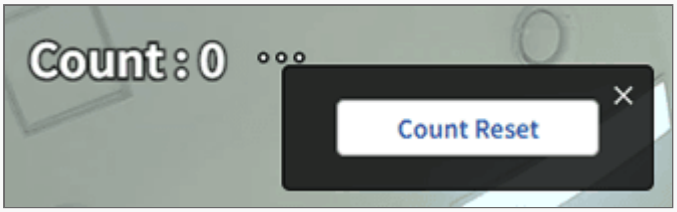
En la sección **Option**, configure las condiciones de activación de eventos y el conteo de eventos.



- **Every Delay**: Establezca la duración mínima para tratarla como un evento. Un evento ocurre solo cuando el estado de detección dura más que el tiempo establecido. Se puede configurar hasta un máximo de 60 segundos.

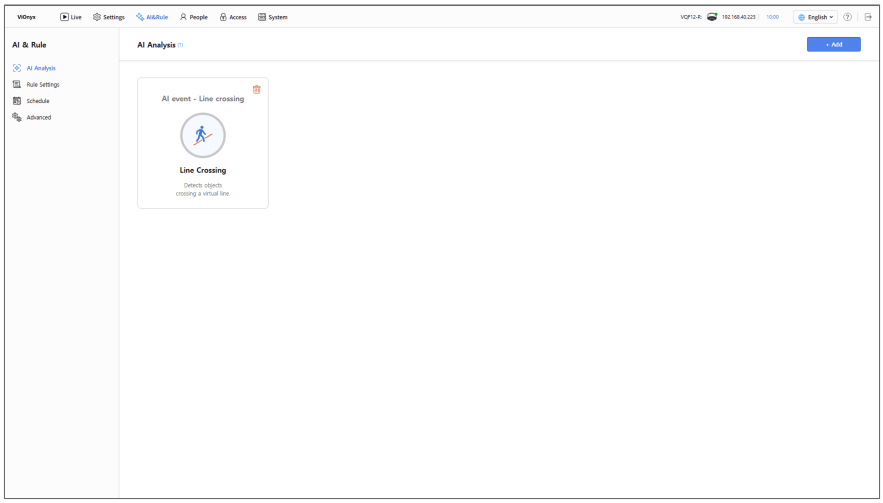
> Si ocurren demasiados eventos, aumente el valor de **Every Delay**. El movimiento detectado por menos del tiempo establecido no se considera un evento, lo que reduce eventos innecesarios.

- **Event Count**: Establezca esta opción en **On** para contar cada cruce de línea. Si existen varias líneas, cuente cada línea por separado.
- **All Event Count Reset**: Establezca esta opción en **On** para inicializar diariamente los conteos de eventos de todas las líneas a la hora especificada. Inicialice los conteos de eventos de todas las líneas a la hora definida en **Reset Time**.

> **Información**
>
> - Si establece **Event Count** en **On**, aparece en el menú **Live** sobre el video de cada línea, en el formato **Count : N**. Haga clic en el botón ••• y seleccione **Count Reset** para inicializar manualmente el conteo de eventos.
>
> 
>
>
> - El firmware versión 1.1.0 o posterior incluye soporte para las opciones de conteo de eventos.

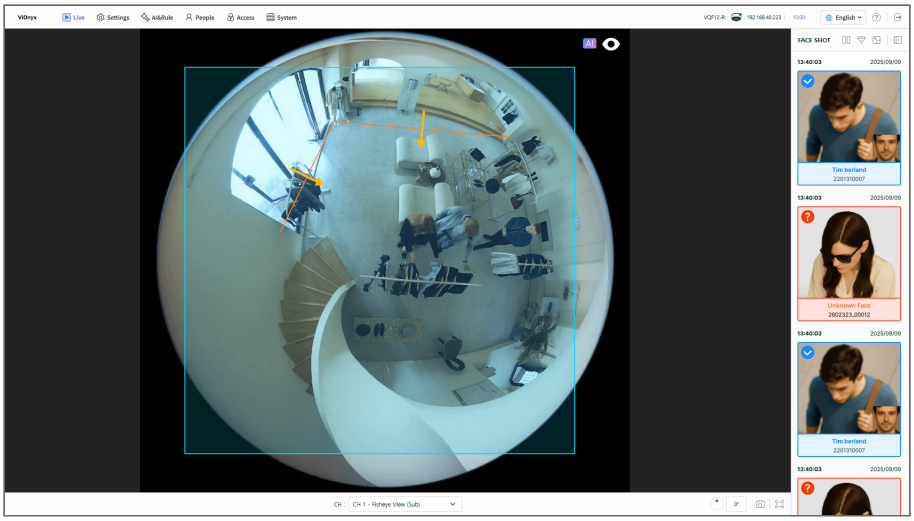
7 Guardar ajustes

Después de completar todas las configuraciones, haga clic en **Create** en la esquina superior derecha. La interfaz vuelve a la pantalla anterior y agrega el nuevo evento de IA a la lista.



Verificar en Live

Haga clic en el menú **Live** en la esquina superior izquierda de la pantalla. Confirme que el ícono AI en la esquina superior derecha de la transmisión de la cámara esté activado. Las líneas virtuales y las áreas faciales configuradas se superponen en el video. Se produce un evento cada vez que una persona cruza una línea virtual. Si configura áreas faciales, la cámara detecta rostros allí; identifica automáticamente a los usuarios enrolados y muestra sus nombres.



Información

- Los usuarios no enrolados aparecen como **Unknown Face**. Los usuarios enrolados aparecen con su nombre.
- La mala iluminación o la luz de fondo pueden impedir que la cámara detecte rostros. Mejore la iluminación del área o ajuste la posición y el ángulo de la cámara para que los rostros se vean con claridad.
- Los rostros deben mirar a la cámara para que la cámara los detecte. Es posible que la cámara no detecte las vistas de perfil o de espaldas.

Configurar Evento de Conteo de Personas

Configure un evento de conteo de personas para detectar la cantidad de personas que permanecen en áreas designadas. Agregue un área facial opcional para autenticar automáticamente a los usuarios enrolados.

¿Cuándo usarlo?

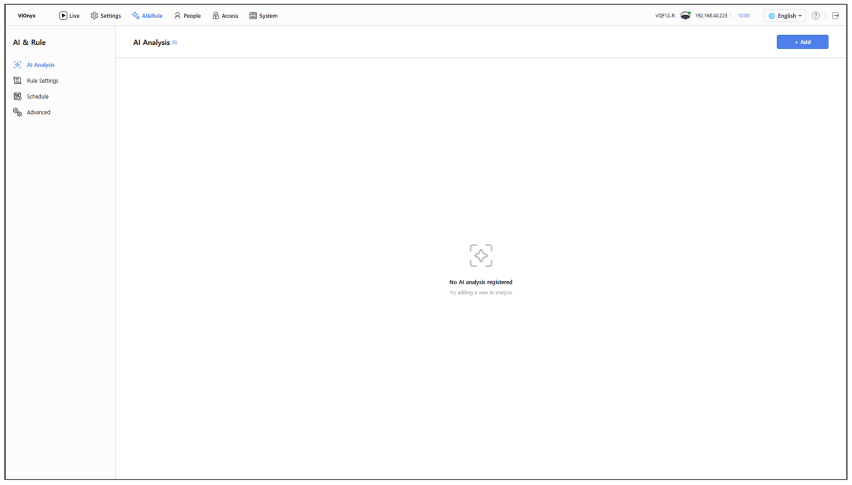
- Cuando necesita monitorear en tiempo real la cantidad de visitantes en una tienda minorista o en un área específica de la tienda.
- Cuando necesita rastrear la cantidad de personas en un área específica para la gestión de multitudes.
- Cuando necesita rastrear el estado de entrada y salida del personal registrado y de clientes VIP.
- Cuando necesita administrar estadísticas de acceso para un área específica por motivos de seguridad.

Crear evento de conteo de personas

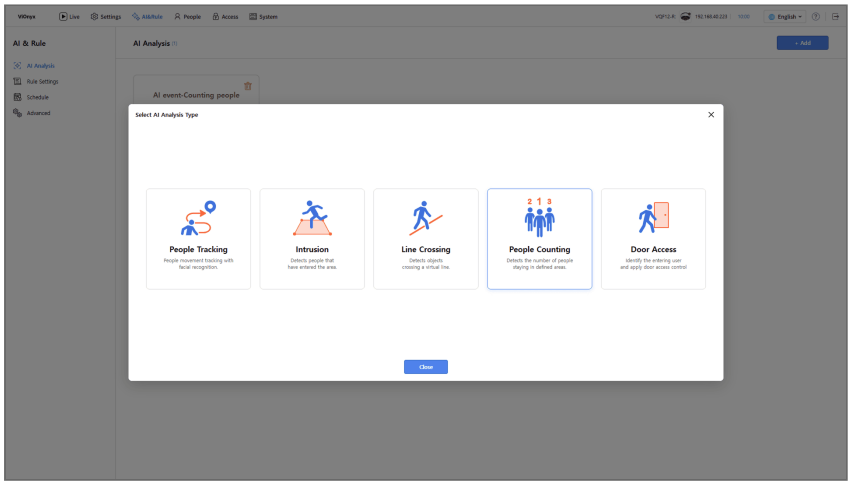
Después de crear un evento de conteo de personas, el menú **Live** detecta la cantidad de personas que permanecen en áreas designadas. Además, al configurar un área facial, se prioriza el seguimiento facial en esa área; los usuarios enrolados se identifican automáticamente.

1 Iniciar creación del evento

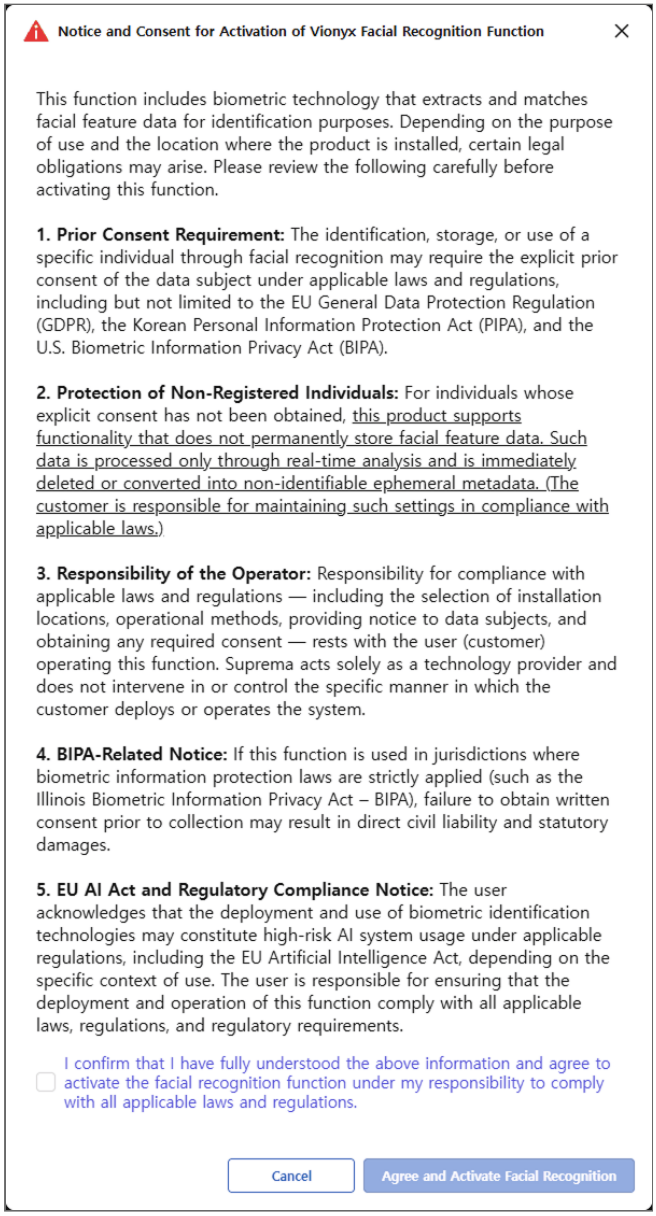
1. Haga clic en el menú **AI&Rule** en la esquina superior izquierda de la pantalla.
2. Haga clic en **AI Analysis** en la barra lateral izquierda.



3. Haga clic en **+ Add** en la esquina superior derecha de la pantalla.
4. Haga clic en **People Counting** en la ventana **Select AI Analysis Type**.

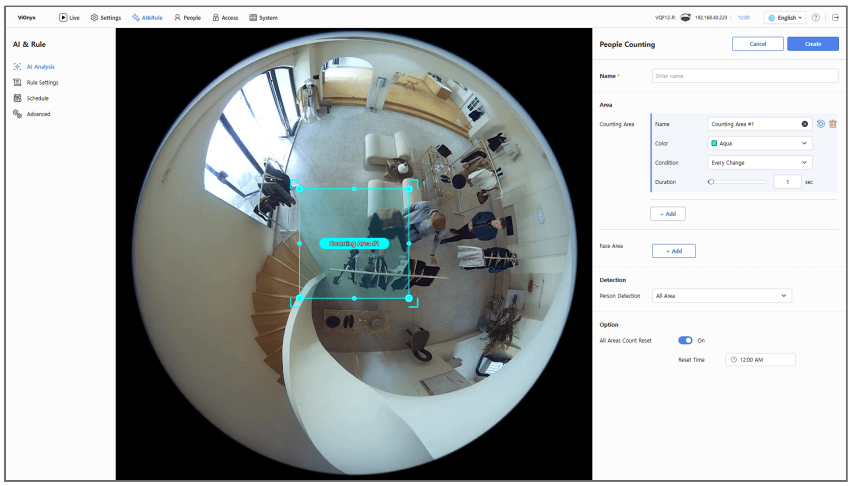


5. Cuando aparece la ventana emergente **Notice and Consent for Activation of Vionyx Facial Recognition Function**, revise los detalles, seleccione la casilla de consentimiento y haga clic en **Agree and Activate Facial Recognition**.



- Para usar la función de Facial Authentication, cumpla con las normas locales. No puede continuar sin consentimiento.
- La ventana emergente **Notice and Consent for Activation of Vionyx Facial Recognition Function** aparece solo una vez. La creación posterior de eventos de IA asume el consentimiento.

6. Complete los ajustes requeridos en el panel derecho **People Counting**.

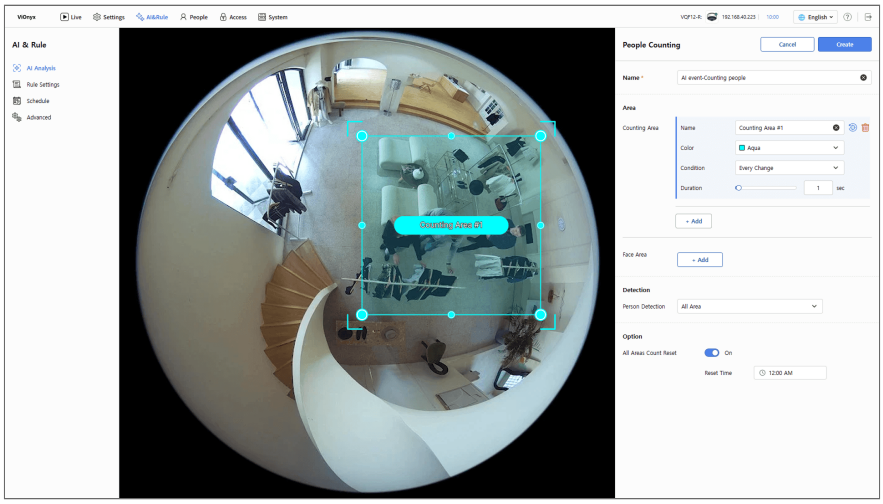


2 Configurar nombre del evento

Ingrese el nombre del evento de IA en el campo **Name**. El nombre puede tener hasta 64 caracteres.

3 Configure el área de conteo

Configure las áreas de conteo en Live View. La cámara cuenta personas dentro de las áreas de conteo configuradas en tiempo real y activa eventos. Configure al menos una línea virtual. Haga clic en **+ Add** para agregar hasta 10. Arrastre las esquinas o los puntos del cuadro del área de conteo en Live View para cambiar su forma. Arrastre el centro para mover la línea.



- **Name**: edite el nombre del área de conteo. Asigne un nombre claro y descriptivo. El nombre del área de conteo aparece al pasar el cursor en Live View.

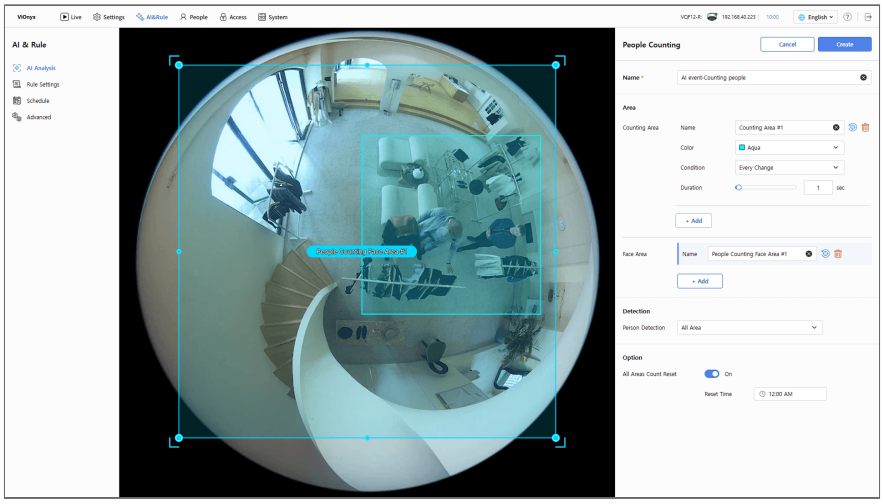
- **Color**: seleccione el color del área de conteo. El área de conteo aparece en el color seleccionado en Live View.
- **Condition**: configure la condición de activación del evento.
  - **Every Change**: active un evento cada vez que una persona entra o sale del área de conteo
  - **Count Limit**: active un evento cuando la cantidad de personas en el área de conteo supere el valor especificado (predeterminado: 10 personas, máximo: 100 personas)
- **Duration**: configure el tiempo mínimo que el conteo en el área de conteo debe cumplir para activar la condición del evento. Por ejemplo, si Duración está configurado en 5 segundos, una persona debe permanecer en el área de conteo al menos 5 segundos para activar el evento. Se puede configurar hasta un máximo de 60 segundos.

Información

- Haga clic en para restablecer la forma y el tamaño del área de conteo configurada.
- Haga clic en para eliminar el área de conteo agregada.

4 Ajustes del área facial (opcional)

Defina el área para la detección facial. Cuando se configura, el sistema prioriza el seguimiento facial en esa área. Las áreas faciales y las áreas de conteo pueden superponerse. Haga clic en **+ Add** para agregar hasta 10 áreas faciales. Aparece un cuadro azul en Live View; arrastre las esquinas o los puntos para ajustar la forma. Arrastre el centro para mover la línea.



- **Name**: edite el nombre del área facial. Asigne un nombre claro y descriptivo. El nombre del área facial aparece al pasar el cursor en Live View.

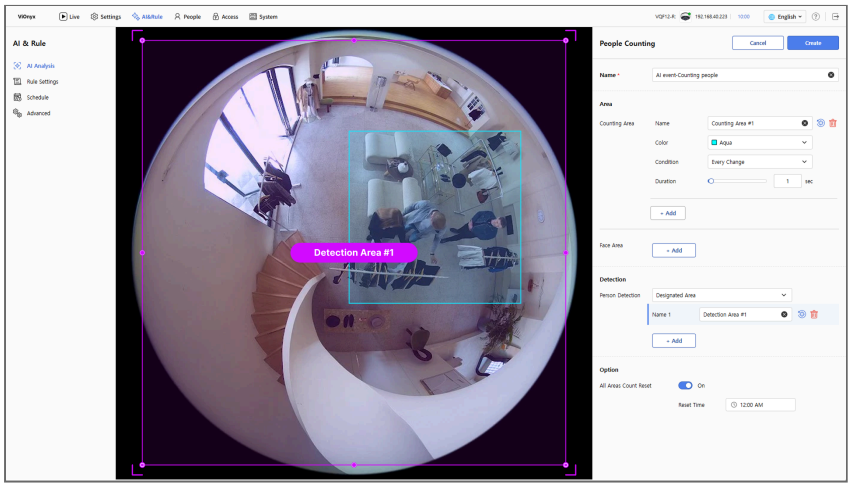
Información

- Los usuarios enrolados se identifican automáticamente en el menú **Live** y se muestran por nombre. Los usuarios no enrolados aparecen como **Unknown Face**.
- Haga clic en para restablecer la forma y el tamaño del área facial configurada.
- Haga clic en para eliminar un área facial agregada.
- En los ajustes de la cámara, si usa la opción **Adaptive AE mode**, ajústela. Haga que el área del rostro incluya el lugar donde una persona se coloca o pasa. Verifique que el rostro aparezca con claridad.

5 Ajustes de detección de personas (opcional)

En la sección **Detection**, seleccione el área donde la cámara detecta personas. Reduzca el área de detección según sea necesario para reducir detecciones falsas en áreas irrelevantes (finales de pasillos, ventanas, superficies reflectantes, etc.).

- **All Area**: Predeterminado. Detecta personas en toda la pantalla. Disponible independientemente de si se establecen áreas faciales.
- **Designated Area**: Detecta personas solo dentro del área que especifique. Disponible solo cuando no se establece un área facial. Configure al menos una línea virtual. Haga clic en **+ Add** para agregar hasta 10. Aparece un cuadro morado en la vista en vivo; arrastre sus esquinas o puntos con el mouse para ajustarlo a la forma deseada. Arrastre el centro para mover la línea.



  - **Name**: Edite el nombre del área de detección de personas.
- **Face Area Only**: Detecta personas solo dentro del área facial. Disponible solo cuando se establece un área facial.

Información

- Al agregar un área facial con **Designated Area** seleccionado, el sistema abre la ventana emergente **Notice**. Haga clic en **OK** para borrar el área de detección designada y cambiar a **Face Area Only**.
- Al eliminar todas las áreas faciales con **Face Area Only** seleccionado, el sistema cambia automáticamente a **All Area**.
- En los ajustes de la cámara, al usar la opción **Adaptive AE mode**, limite el rango a **Designated Area** o **Face Area Only**. Mantenga pantallas, fotos o pósteres con rostros fuera del área de detección.
- Haga clic en para inicializar la forma y el tamaño del área de detección de personas.
- Haga clic en para eliminar el área de detección de personas agregada.
- La versión de firmware 1.1.0 o posterior incluye soporte para esta característica.

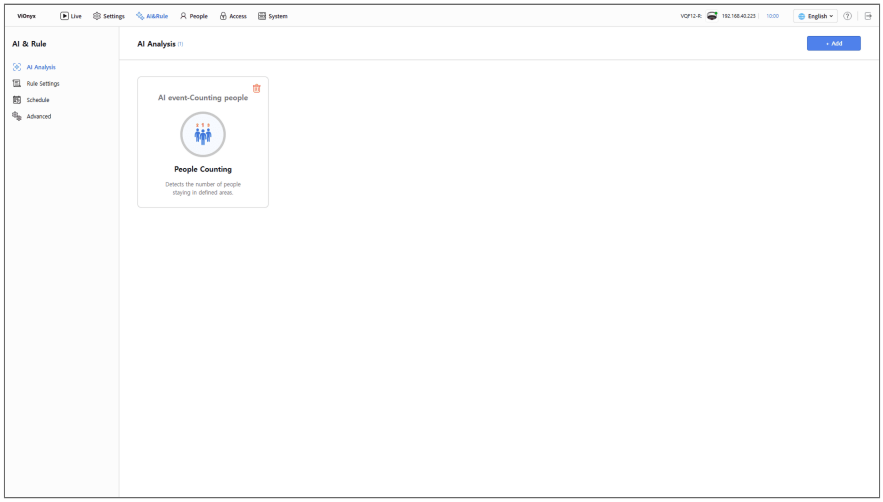
6 Ajustes de restablecimiento del conteo

Configure la condición para restablecer el conteo de personas en las áreas de conteo.

- **All Areas Count Reset**: configúrelo en **On** para restablecer los conteos de todas las áreas de conteo en la hora programada. El sistema restablece los conteos de todas las áreas de conteo a la hora configurada en **Reset Time**.

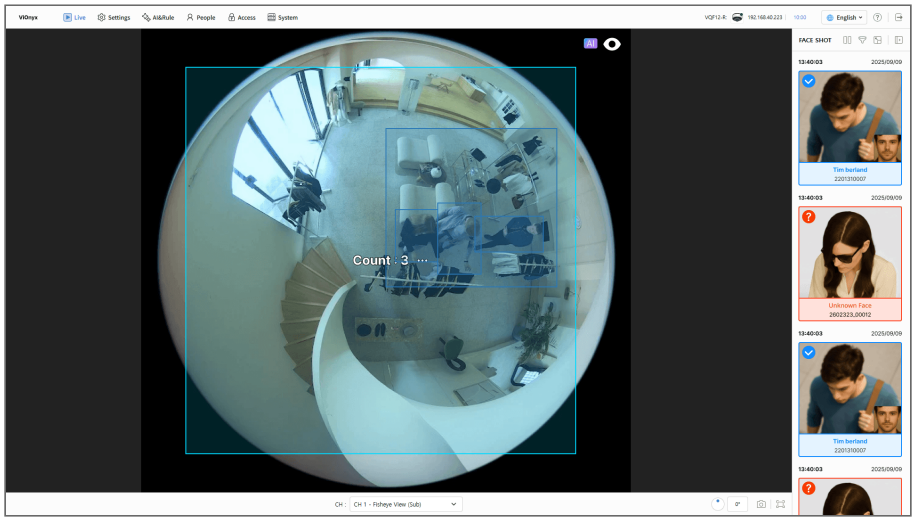
7 Guardar ajustes

Después de completar todas las configuraciones, haga clic en **Create** en la esquina superior derecha. La interfaz vuelve a la pantalla anterior y agrega el nuevo evento de IA a la lista.



Verificar en Live

Haga clic en el menú **Live** en la esquina superior izquierda de la pantalla. Confirme que el ícono AI en la esquina superior derecha de la transmisión de la cámara esté activado. Las áreas de conteo y faciales configuradas aparecen como superposiciones en el video. Muestra la cantidad de personas en el área de conteo con el formato **Count : N**. Si configura áreas faciales, la cámara detecta rostros allí; identifica automáticamente a los usuarios enrolados y muestra sus nombres.



Información

- Para restablecer el conteo manualmente, haga clic en ••• → **Count Reset**.



- Los usuarios no enrolados aparecen como **Unknown Face**. Los usuarios enrolados aparecen con su nombre.
- La mala iluminación o la luz de fondo pueden impedir que la cámara detecte rostros. Mejore la iluminación del área o ajuste la posición y el ángulo de la cámara para que los rostros se vean con claridad.
- Los rostros deben mirar a la cámara para que la cámara los detecte. Es posible que la cámara no detecte las vistas de perfil o de espaldas.

Configurar Eventos De Control De Acceso

Los eventos de control de acceso identifican con autenticación facial, verifican personas cercanas y deciden el acceso. Detecte el tailgating, cuando una persona no autorizada sigue a un usuario autenticado, y excluya a las personas que salen por la puerta de la evaluación.

Información

La versión de firmware 1.1.0 o posterior incluye soporte para eventos de control de acceso.

¿Cuándo usarlo?

- Cuando la autenticación facial verifica si la persona que se acerca a la puerta está inscrita
- Cuando deba evitar tailgating: una persona no autorizada sigue a un usuario autenticado al entrar
- Cuando evalúe solo las entradas y excluya a quienes salen desde el interior
- Al vincular acciones posteriores, como abrir la puerta o mostrar un aviso de advertencia, según la decisión

Información

Los eventos de control de acceso solo **determinan** si permiten el acceso y no controlan directamente el relé de la puerta. Para abrir la puerta según los resultados, cree un evento, agregue la puerta y vincule el evento. Para acciones adicionales, como indicaciones de voz o notificaciones por webhook, configure reglas de puertas.

- Para obtener más información sobre el registro y la gestión de puertas, consulte Administrar Puertas.
- Para obtener más información sobre las reglas de puertas, consulte Configurar Reglas de Puerta.

Cómo funcionan los eventos de control de acceso

Los eventos de control de acceso deciden si permiten el acceso al combinar los siguientes elementos. Antes de iniciar la configuración, revise el rol de cada elemento.

Componente	roles	Obligatorio
Validation Area	Es un área más amplia que rodea la zona de control de acceso. Verifique la cantidad de personas y el estado de identificación en esta área para detectar tailgating.	Si
Door Access Area	Es el área justo frente a la puerta. Cuando una persona entra en esta área, el sistema lo considera un intento de acceso e inicia la evaluación.	Si
Event Entry Line	Esta línea determina quién cruza la puerta de acceso. Según la dirección seleccionada, el sistema determina la entrada, la salida o ambas.	Si
Face Area	Es el área donde el sistema rastrea primero los rostros para identificar usuarios.	Opción

La cámara clasifica a las personas en la zona en uno de los siguientes estados.

- **Identificado**: La autenticación facial se completó correctamente y la persona coincide con un usuario enrolado.
- **No identificado**: La autenticación facial falló o la persona no coincide con un usuario enrolado. El menú En vivo muestra a personas no enroladas, con el rostro cubierto o que no miran a la cámara como **Unknown Face**.

Precaución

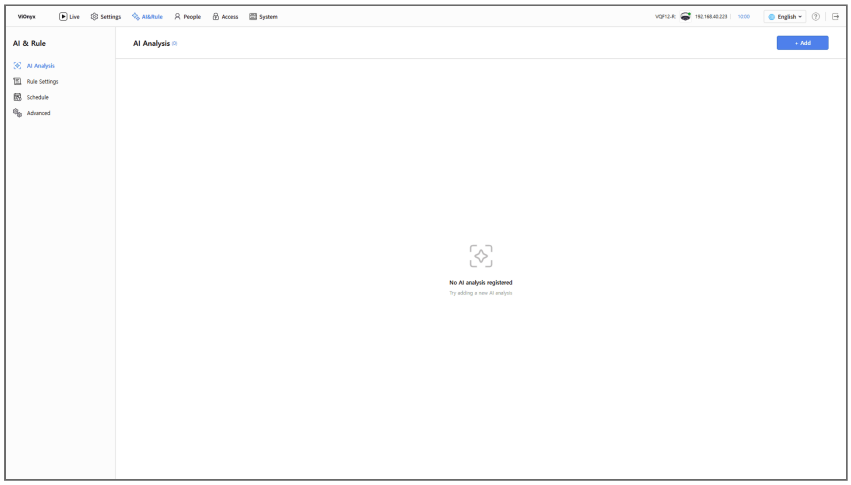
Por seguridad, el sistema no trata a una persona no reconocida como usuario autenticado. Si una persona no se identifica en el área de control de acceso, el sistema deniega el acceso.

Crear evento de control de acceso

Un evento de control de acceso identifica a los usuarios en el menú **Live**. También verifica a quienes ingresan detrás.

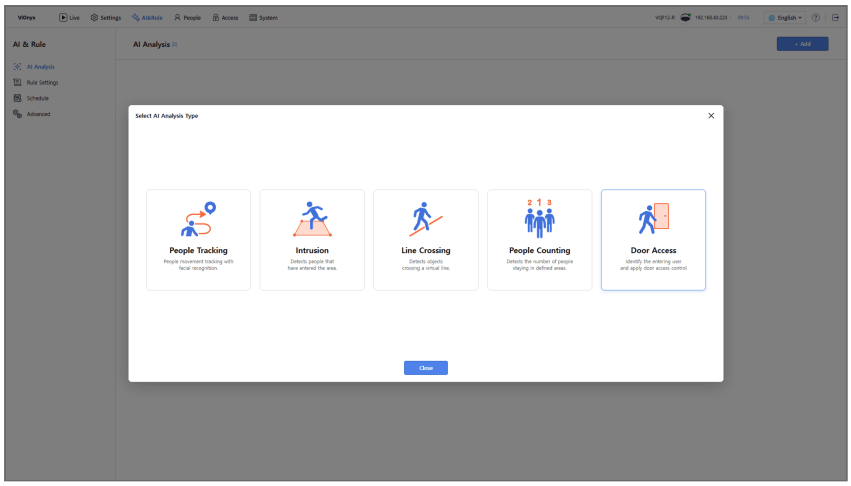
1 Iniciar creación del evento

1. Haga clic en el menú **AI&Rule** en la esquina superior izquierda de la pantalla.
2. Haga clic en **AI Analysis** en la barra lateral izquierda.

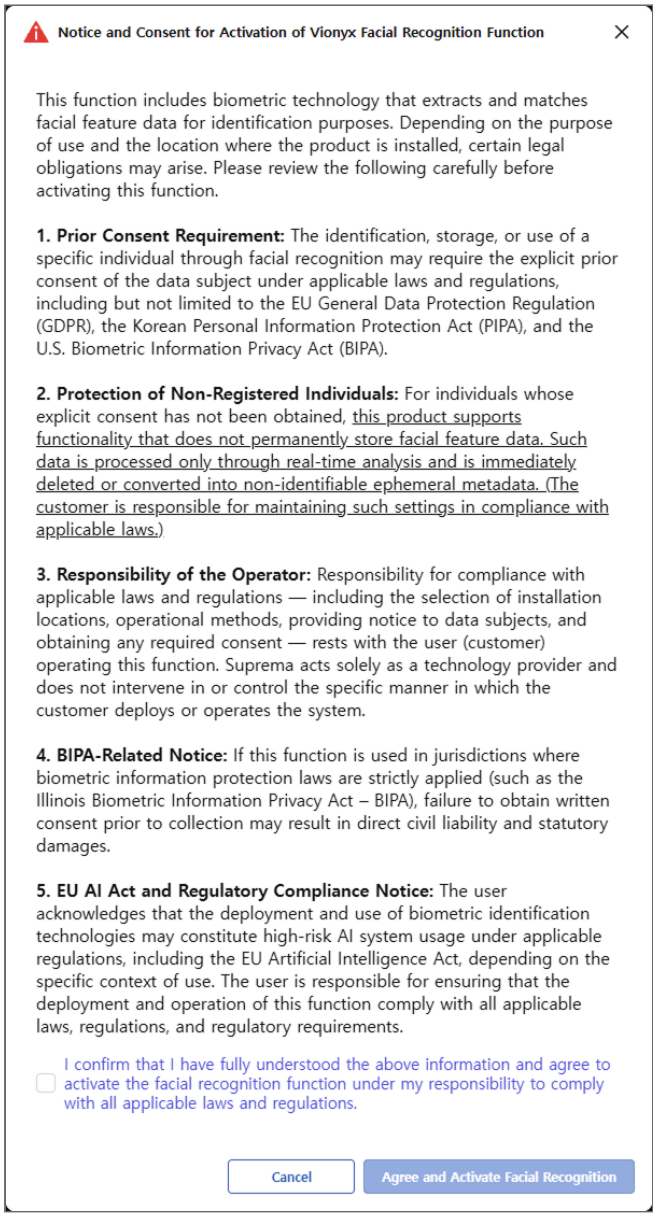


3. Haga clic en **+ Add** en la esquina superior derecha de la pantalla.

4. En la ventana **Select AI Analysis Type**, haga clic en **Door Access**.

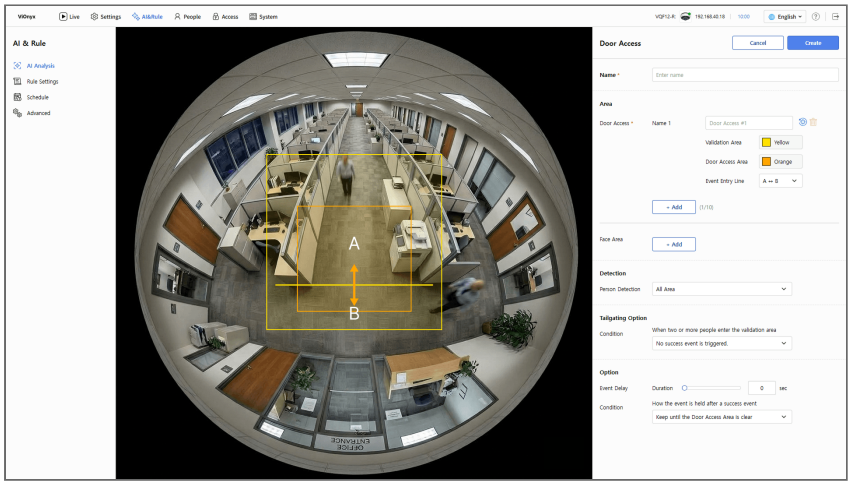


5. Cuando aparece la ventana emergente **Notice and Consent for Activation of Vionyx Facial Recognition Function**, revise los detalles, seleccione la casilla de consentimiento y haga clic en **Agree and Activate Facial Recognition**.



- El evento de control de acceso usa autenticación facial para identificar usuarios. Acepte usarla antes de crearlo.
- Para usar la función de Facial Authentication, cumpla con las normas locales.
- La ventana emergente **Notice and Consent for Activation of Vionyx Facial Recognition Function** aparece solo una vez. La creación posterior de eventos de IA asume el consentimiento.

6. Complete los ajustes requeridos en el panel **Door Access** de la derecha.

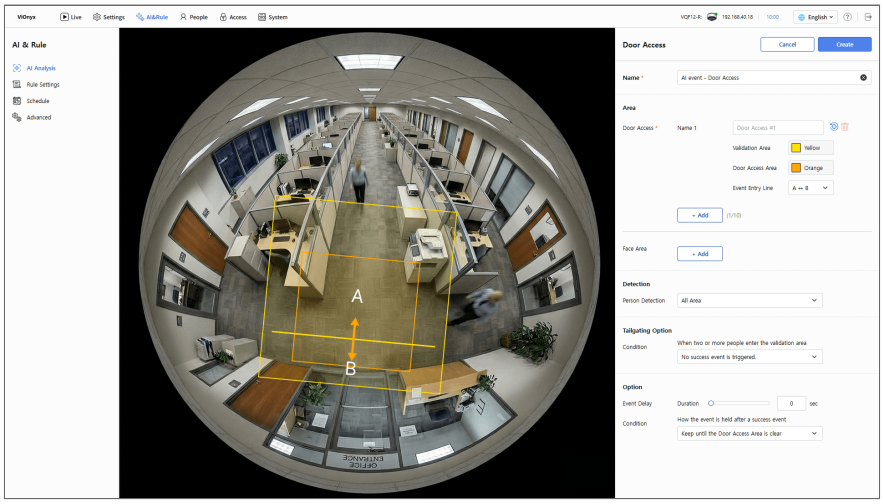


2 Configurar nombre del evento

Ingrese el nombre del evento de IA en el campo **Name**. El nombre puede tener hasta 64 caracteres.

3 Ajustes del área de control de acceso

En la sección **Area**, defina el área de validación, el área de control de acceso y la línea de entrada del evento para la ubicación de la puerta. Configure al menos una línea virtual. Haga clic en **+ Add** para agregar hasta 10. Cada vez que lo agregue, la vista en vivo muestra los tres elementos como un conjunto. Arrastre las esquinas o los puntos para ajustar la forma, y arrastre el área central para moverla.



- **Name**: Edite el nombre del área de control de acceso. Use un nombre claro, como la ubicación de la puerta.
- **Validation Area**(Amarillo): Área de validación que rodea el área de control de acceso. Defínala más amplia que el área de control de acceso para detectar aproximaciones rápidas y personas que se cuelan.
- **Door Access Area**(Naranja): Defínala justo frente a la puerta, por donde la persona debe pasar para ingresar. Cuando una persona ingresa en esta área, el sistema determina el acceso.
- **Event Entry Line**: Esta línea determina quién cruza la puerta de acceso. Arrastre los puntos de ambos extremos para colocar la línea a través del área de control de acceso. Luego, seleccione la dirección de cruce.
  - **A → B**: Detecte solo a las personas que crucen de A a B.

– **B → A**: Detecte solo a las personas que crucen de B a A.

– **A ↔ B**: Detecte ambas direcciones. El sistema distingue entre las personas que entran y las que salen.

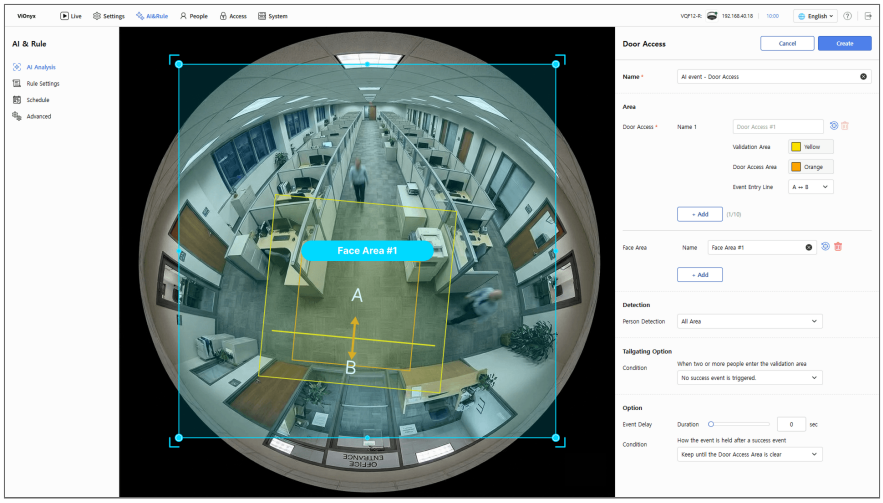
Para detectar solo una dirección, verifique las posiciones de A y B en la Vista en vivo y luego seleccione **A → B** o **B → A**.

Información

- El área de validación debe incluir por completo el área de control de acceso. El sistema no guarda si el área de control de acceso se extiende fuera del área de validación.
- Extienda la línea de entrada del evento más allá del área de control de acceso, pero manténgala dentro del área de verificación.
- Para inicializar la forma y el tamaño del área configurada, haga clic en .
- Para eliminar el área de control de acceso agregada, haga clic en .

4 Ajustes del área facial (opcional)

Defina el área para la detección facial. Al activarla, el sistema prioriza el seguimiento facial en esa área para identificar a los usuarios. Establezca el área facial donde una persona que se acerca a la puerta se vea claramente de frente. Las áreas faciales y las áreas de control de acceso pueden superponerse. Haga clic en **+ Add** para agregar hasta 10 áreas faciales. Aparece un cuadro azul en Live View; arrastre las esquinas o los puntos para ajustar la forma. Arrastre el centro para mover la línea.



- **Name**: edite el nombre del área facial. Asigne un nombre claro y descriptivo. El nombre del área facial aparece al pasar el cursor en Live View.

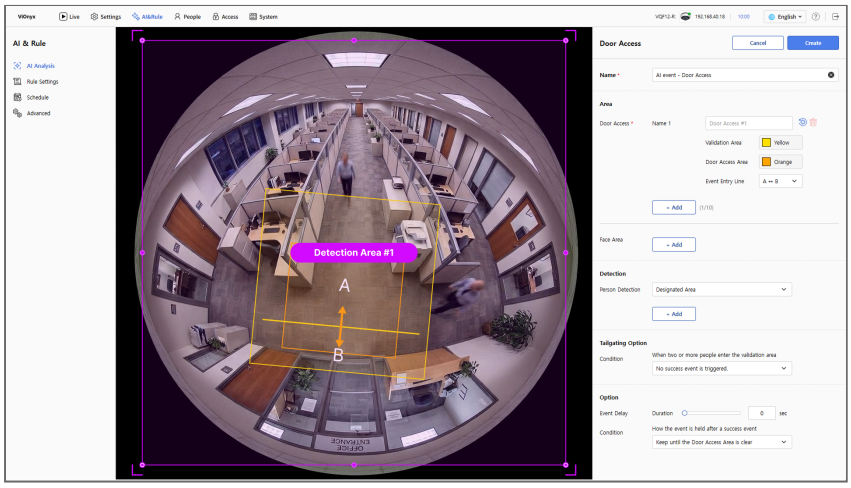
Información

- Los usuarios enrolados se identifican automáticamente en el menú **Live** y se muestran por nombre. Los usuarios no enrolados aparecen como **Unknown Face**.
- Haga clic en para restablecer la forma y el tamaño del área facial configurada.
- Haga clic en para eliminar un área facial agregada.
- En los ajustes de la cámara, si usa la opción **Adaptive AE mode**, ajústela. Haga que el área del rostro incluya el lugar donde una persona se coloca o pasa. Verifique que el rostro aparezca con claridad.

5 Ajustes de detección de personas (opcional)

En la sección **Detection**, seleccione el área donde la cámara detecta personas. Reduzca el área de detección según sea necesario para reducir detecciones falsas en áreas irrelevantes (finales de pasillos, ventanas, superficies reflectantes, etc.).

- **All Area**: Predeterminado. Detecta personas en toda la pantalla. Disponible independientemente de si se establecen áreas faciales.
- **Designated Area**: Detecta personas solo dentro del área que especifique. Disponible solo cuando no se establece un área facial. Configure al menos una línea virtual. Haga clic en **+ Add** para agregar hasta 10. Aparece un cuadro morado en la vista en vivo; arrastre sus esquinas o puntos con el mouse para ajustarlo a la forma deseada. Arrastre el centro para mover la línea.



  - **Name**: Edite el nombre del área de detección de personas.
- **Face Area Only**: Detecta personas solo dentro del área facial. Disponible solo cuando se establece un área facial.

Información

- Al agregar un área facial con **Designated Area** seleccionado, el sistema abre la ventana emergente **Notice**. Haga clic en **OK** para borrar el área de detección designada y cambiar a **Face Area Only**.
- Al eliminar todas las áreas faciales con **Face Area Only** seleccionado, el sistema cambia automáticamente a **All Area**.
- En los ajustes de la cámara, al usar la opción **Adaptive AE mode**, limite el rango a **Designated Area** o **Face Area Only**. Mantenga pantallas, fotos o pósteres con rostros fuera del área de detección.
- Haga clic en  para inicializar la forma y el tamaño del área de detección de personas.
- Haga clic en  para eliminar el área de detección de personas agregada.
- La versión de firmware 1.1.0 o posterior incluye soporte para esta característica.

6 Ajustes de la opción de tailgating

En la sección **Tailgating Option**, seleccione cómo determina el sistema el acceso cuando hay 2 o más personas en el área de verificación. Las opciones se enumeran de mayor a menor seguridad.

- **No success event is triggered.**: Si hay 2 o más personas en el área de verificación, el sistema deniega el acceso, independientemente de los resultados de identificación. Esta opción es adecuada para áreas donde solo debe pasar una persona a la vez.
- **Success event only when all individuals are valid.**: El sistema autoriza el acceso solo cuando identifica a todos en el área de verificación como usuarios inscritos. El sistema deniega el acceso si alguien permanece sin identificar.
- **Success event if any identified individual is valid.**: El sistema autoriza el acceso si al menos un usuario inscrito está en el área de verificación. Esta opción autoriza el acceso con personas sin identificar. Es adecuada para áreas con visitantes escoltados frecuentes.
- **No effect on event triggering.**: El sistema ignora el conteo de personas en el área de verificación. Basa el acceso solo en el resultado de identificación de la persona que ingresa.

Lo siguiente muestra la decisión de cada opción cuando un usuario inscrito ingresa con otras personas en el área de verificación.

Opción	Cuando solo estén presentes usuarios con permisos de acceso válidos	Cuando la lista incluya usuarios con permisos de acceso inválidos
No success event is triggered.	Acceso denegado	Acceso denegado
Success event only when all individuals are valid.	Acceso autorizado	Acceso denegado
Success event if any identified individual is valid.	Acceso autorizado	Acceso autorizado

Opción	Cuando solo estén presentes usuarios con permisos de acceso válidos	Cuando la lista incluya usuarios con permisos de acceso inválidos
No effect on event triggering.	Acceso autorizado	Acceso autorizado

Consejo
Para puertas críticas para la seguridad, use **Success event only when all individuals are valid.** o superior.

7 Establecer condiciones de activación de eventos

En la sección **Option**, establezca las condiciones de activación del evento.

- **Event Delay**: Establezca la duración mínima para tratarlo como un evento. Un evento ocurre solo cuando el estado de detección dura más que el tiempo establecido. Se puede configurar hasta un máximo de 60 segundos.

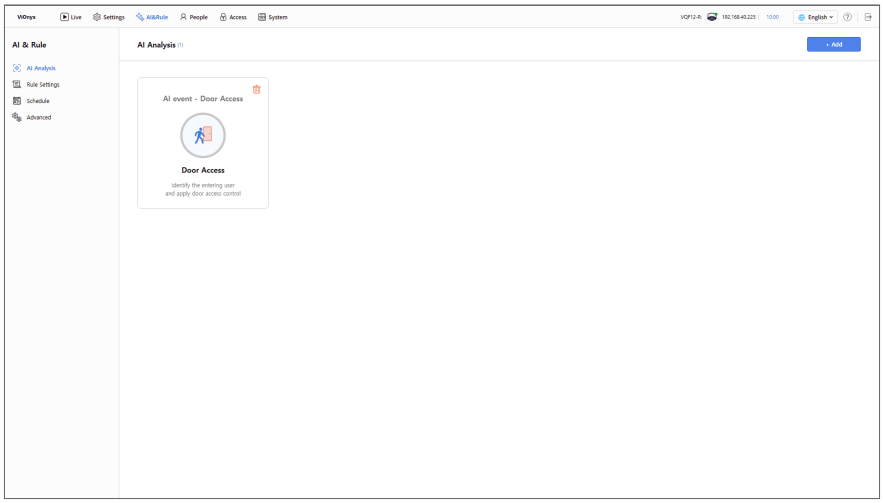
  Si los eventos ocurren con demasiada frecuencia porque las personas pasan brevemente frente a la puerta, aumente el valor de **Event Delay**. El movimiento detectado por menos del tiempo establecido no se considera un evento, lo que reduce eventos innecesarios.

- **Condition**: Seleccione cuánto tiempo mantener el evento después de conceder el acceso. Mientras el evento permanezca activo, las acciones vinculadas (por ejemplo, abrir la puerta) también permanecen activas.
  - **Keep until the Door Access Area is clear**: Mantenga el evento hasta que no quede nadie en el área con control de acceso. La puerta permanece abierta mientras el usuario autenticado esté frente a ella, sin volver a autenticarse.
  - **Keep until the area is clear or a tailgating violation occurs**: Finalice el evento cuando el área quede vacía. Finalícelo de inmediato cuando una persona no autorizada ingrese al área de verificación y viole el ajuste de tailgating. Esto evita que personas no autorizadas sigan a alguien mientras la puerta está abierta.
  - **Trigger once on entry (no hold)**: No mantenga el evento. Actívelo una vez cada vez que alguien ingrese al área con control de acceso.

Información
Si un usuario inscrito duda frente a la puerta y no puede entrar, la puerta se abre solo después de salir y volver a ingresar al área con control de acceso. Para reducir esta molestia y mantener la seguridad, seleccione **Keep until the area is clear or a tailgating violation occurs**.

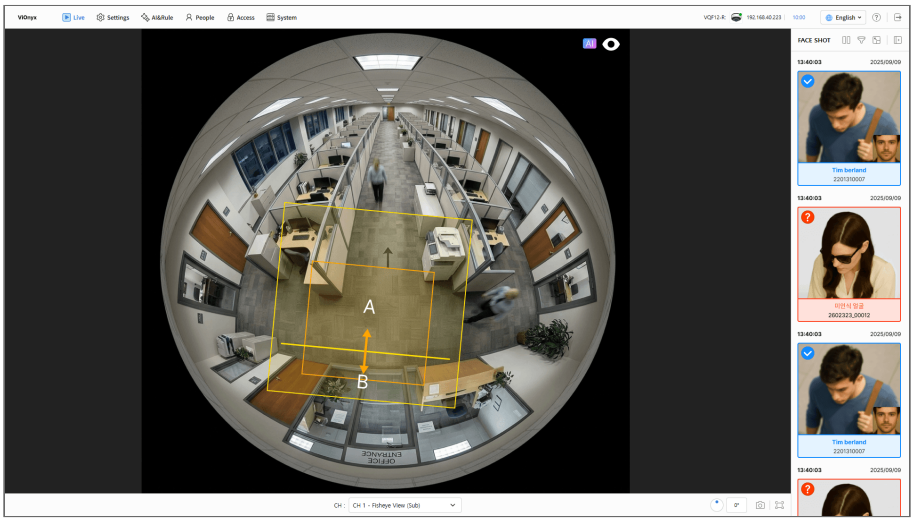
8 Guardar configuración

Después de completar todas las configuraciones, haga clic en **Create** en la esquina superior derecha. La interfaz vuelve a la pantalla anterior y agrega el nuevo evento de IA a la lista.



Verificar en Live

Haga clic en el menú **Live** en la esquina superior izquierda de la pantalla. Confirme que el ícono AI en la esquina superior derecha de la transmisión de la cámara esté activado. El área de verificación definida, el área con control de acceso, la línea de entrada del evento y el área facial aparecen como superposiciones en el video. Cuando alguien ingresa al área con control de acceso, el sistema activa Acceso concedido o Acceso denegado según la identificación y las opciones de tailgating.



Información

- Los usuarios no enrolados aparecen como **Unknown Face**. Los usuarios enrolados aparecen con su nombre.
- La mala iluminación o la luz de fondo pueden impedir que la cámara detecte rostros. Mejore la iluminación del área o ajuste la posición y el ángulo de la cámara para que los rostros se vean con claridad.
- Los rostros deben mirar a la cámara para que la cámara los detecte. Es posible que la cámara no detecte las vistas de perfil o de espaldas. Si el sistema no puede identificar un rostro, trata a la persona como no identificada y deniega el acceso.

Siguiente paso

El evento de control de acceso solo determina si se permite el acceso. Defina reglas de la puerta para ejecutar acciones adicionales, como mensajes de voz, notificaciones webhook o luces de advertencia.

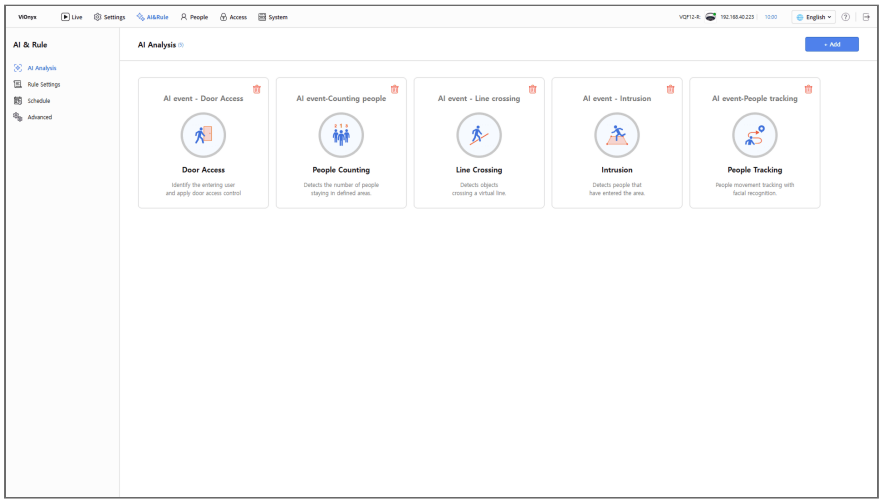
Después de crear un evento de control de acceso, agregue la puerta y vincule el evento. Cuando el sistema concede el acceso, el relé conectado a la puerta se activa y la abre.

Editar y Eliminar Eventos de IA

Modifique la configuración de los eventos de IA creados o elimine los eventos que ya no necesita.

Editar configuración del evento de IA

1. Haga clic en el menú **AI&Rule** en la esquina superior izquierda de la pantalla.
2. Haga clic en **AI Analysis** en la barra lateral izquierda.



3. Haga clic en el evento de IA que desea editar.
4. En el panel derecho, edite la configuración del evento de IA.
5. Después de terminar toda la configuración, haga clic en **Update** en la esquina superior derecha.

Regrese a la pantalla anterior y confirme el evento modificado en la lista de eventos de IA.

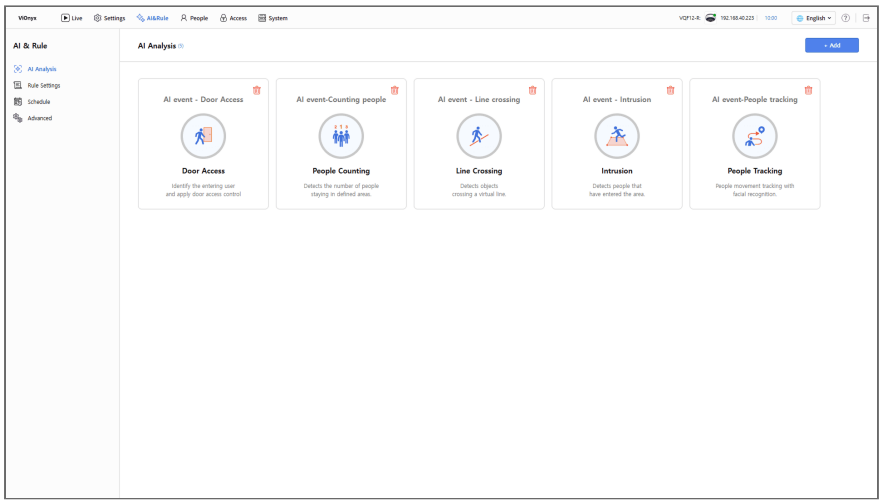
Información

Para obtener más información sobre cada configuración del evento, consulte el siguiente documento.

- Configurar Eventos de Seguimiento de Personas
- Configurar Eventos de Detección de Intrusión
- Configurar Evento de Detección de Cruce de Línea
- Configurar Evento de Conteo de Personas
- Configurar Eventos De Control De Acceso

Eliminar evento de IA

1. Haga clic en el menú **AI&Rule** en la esquina superior izquierda de la pantalla.
2. Haga clic en **AI Analysis** en la barra lateral izquierda.



3. Haga clic en a la derecha del evento de IA que desea eliminar.
4. Cuando aparezca un mensaje de advertencia, revise el mensaje y haga clic en **OK**.

Información

- Los eventos de IA eliminados no se pueden recuperar. Si un evento de IA está vinculado a reglas (Rule), al eliminar el evento también se eliminan las reglas vinculadas.
- Eliminar un evento de IA registra la eliminación en el registro del sistema.

Ajustes de Reglas de IA

Use reglas de IA para reproducir audio automáticamente, enviar webhooks o activar acciones de relé según el tipo de evento y las condiciones. Este documento guía el procedimiento completo para crear y operar reglas.

Configure reglas de IA en las siguientes situaciones.

- Envíe un webhook a un servidor externo cuando ocurra un evento específico de IA.

- Reproduzca audio en el dispositivo cuando ocurra un evento específico de IA.
- Active un relé conectado a una puerta de acceso cuando ocurra un evento de IA específico
- Automatice diferentes acciones de seguimiento según el tipo de evento.

Antes de comenzar

Antes de empezar la configuración de reglas, revise lo siguiente.

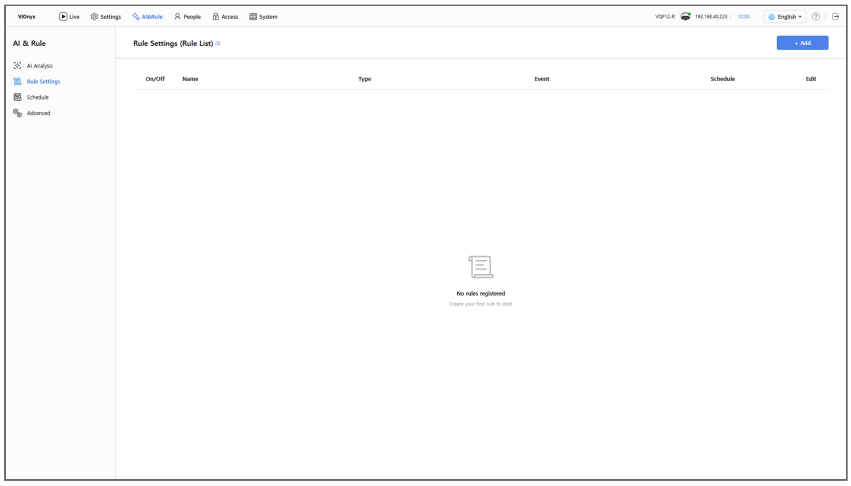
- Los eventos de IA ya deben existir. Consulte los siguientes documentos para crear eventos de IA.
  - Configurar Eventos de Seguimiento de Personas
  - Configurar Eventos de Detección de Intrusión
  - Configurar Evento de Detección de Cruce de Línea
  - Configurar Evento de Conteo de Personas
- Prepare los clips de audio que se reproducirán antes de usar audio.
- Prepare con antelación la URL del receptor del webhook.
- Al usar relés, verifique que el puerto de relé del dispositivo o subdispositivo esté conectado.
- Configure al menos una acción: audio, webhook o relé.

> **Información**
> En eventos de IA, **Door Access** no puede utilizarse como condición para reglas de IA.

Crear regla de IA

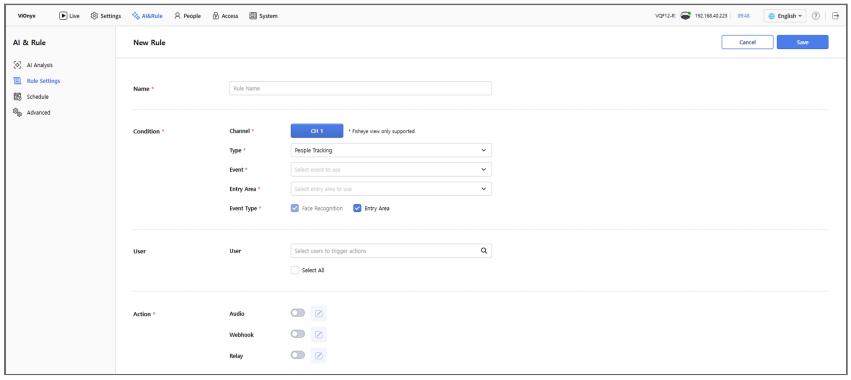
1 Iniciar la creación de una regla

1. Haga clic en el menú **AI&Rule** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Rule Settings** en la barra lateral izquierda.



3. Haga clic en **+ Add** en la esquina superior derecha de la pantalla.

4. Cuando aparezca la pantalla **New Rule**, ingrese el nombre de la regla y configure las condiciones y acciones.



2 Ingresar nombre de la regla

Ingrese el nombre de la regla en el campo de entrada **Name**. El nombre de la regla es obligatorio. Hasta 64 caracteres.

3 Configurar condiciones

Las condiciones determinan si una regla se ejecuta cuando ocurre un evento de IA. En la sección **Condition**, configure las condiciones según se indica a continuación. Las opciones **Type** y **Event** aparecen según la configuración especificada al crear el evento de IA.

- **Channel**: El canal está fijo en CH 1. Solo se admite la vista Fisheye.
- **Type**: Seleccione el tipo de evento de IA. Seleccione una de las siguientes opciones.
  - **People Tracking**
  - **Intrusion**
  - **Line Crossing**
  - **People Counting**
- **Event**: Seleccione el evento de IA que activará la regla. La lista de eventos muestra los eventos de IA que coinciden con el tipo seleccionado. Los eventos aparecen en el formato `(ID:N) event_name`.
- **Entry Area** / **Intrusion Area** / **Line** / **Counting Area**: Agregue condiciones para un área según el tipo de evento seleccionado.
- **Event Type**: Seleccione el tipo de evento que determina si la regla se ejecuta. La regla se ejecuta según el tipo de evento seleccionado.

> Debe seleccionar al menos un tipo de evento.

4 Selección de usuario

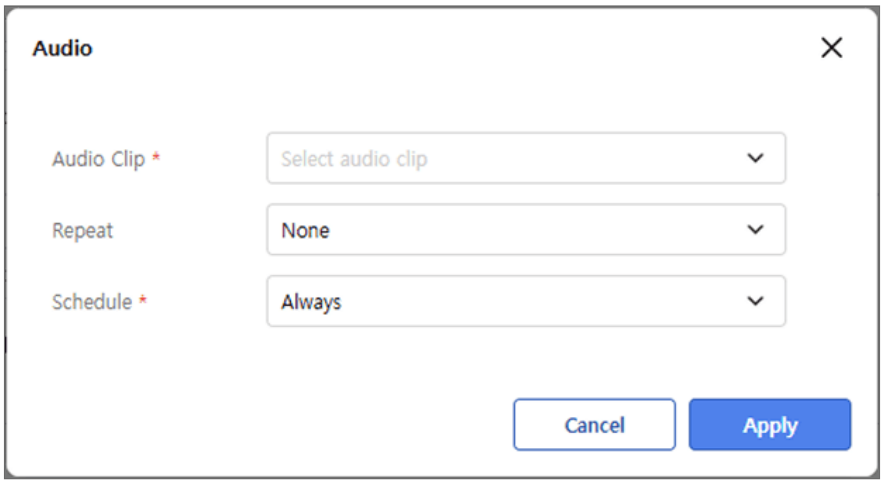
En la sección **User**, seleccione el usuario que determina si la regla se ejecuta. El sistema ejecuta la regla cuando detecta

al usuario seleccionado en un evento de IA.

- Haga clic en **Select users to trigger actions** para seleccionar usuarios específicos. Cuando aparezca la lista de usuarios, seleccione los usuarios deseados y haga clic en el botón **Save**.
- Haga clic en **Select All** para seleccionar a todos los usuarios registrados.

5 Ajustes de acción de audio

La acción de audio reproduce audio de la cámara cuando ocurre un evento de IA. En la sección **Action**, haga clic en el interruptor **Audio** para activar la acción y, luego, haga clic en . Aparece la ventana emergente de ajustes de audio.



- **Audio Clip**: Seleccione el clip de audio que se reproducirá. Seleccione un clip de audio de la lista de clips cargados en el sistema.
- **Repeat**: Configure la cantidad de veces que se repetirá la reproducción de audio. Reproduce el clip de audio repetidamente la cantidad de veces que configure. Puede configurarse hasta un máximo de 10 veces.
- **Schedule**: Seleccione el horario en que la regla se ejecuta y reproduce audio.

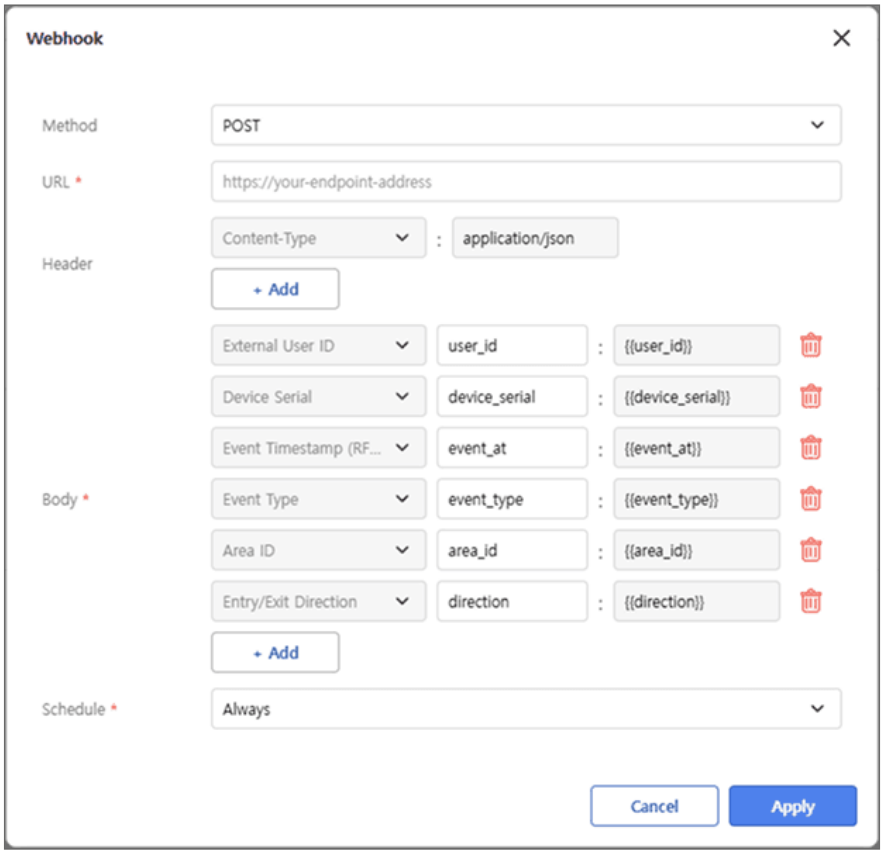
Haga clic en **Apply** para guardar los ajustes de la acción de audio.

Información

- Prepare los clips de audio antes de configurar acciones de audio. Cargue clips de audio en **System** → **Audio**. Para obtener más información, consulte Subir Clips de Audio.
- Cree, edite o elimine horarios en **AI&Rule** → **Schedule**. Para más información sobre la gestión de horarios, consulte Administrar horarios.

6 Ajustes de acción de webhook

La acción de webhook envía un webhook a un servidor externo cuando ocurre un evento de IA. En la sección **Action**, haga clic en el interruptor **Webhook** para activar la acción y, luego, haga clic en . Aparece la ventana emergente de ajustes de webhook.



- **Method**: El método de transmisión del webhook. Solo se admite el método `POST`.
- **URL**: Ingrese la URL para recibir el webhook. La dirección debe ser válida y comenzar con `http://` o `https://`.
- **Header**: Configure los encabezados HTTP que se incluirán en el webhook. Haga clic en **+ Add** para agregar encabezados. Ingrese cada encabezado como un par clave-valor.
- **Body**: Configure el cuerpo HTTP que se incluirá en el webhook. Haga clic en **+ Add** para agregar elementos del cuerpo. Ingrese cada elemento del cuerpo como un par clave-valor.
- **Schedule**: Seleccione el horario en que la regla se ejecuta y envía webhooks.

Haga clic en el botón **Apply** para guardar los ajustes de la acción de webhook.

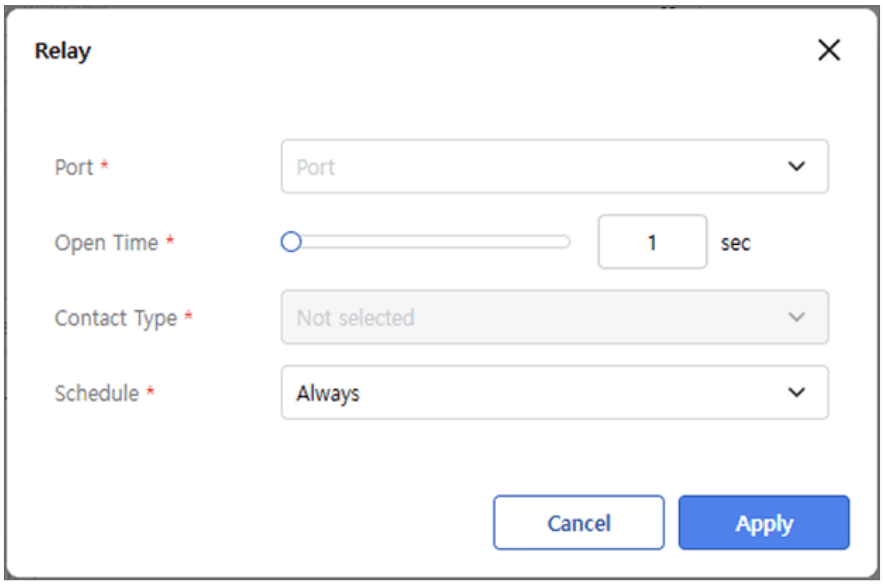
> **Información**
>
> - Los registros de envío del webhook y los códigos de respuesta se pueden revisar en los registros del sistema para solucionar problemas.
> - Cree, edite o elimine horarios en **AI&Rule** → **Schedule**. Para más información sobre la gestión de horarios, consulte Administrar horarios.

7 Ajustes de la acción de relé

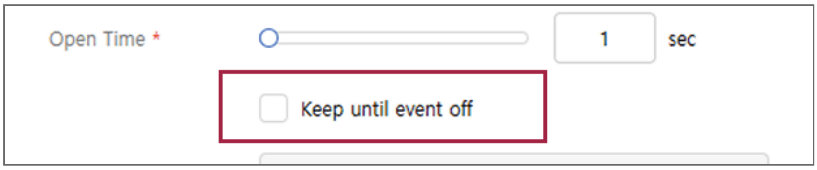
La característica de acción de relé activa el relé en el dispositivo o subdispositivo cuando ocurre un evento de IA. Por ejemplo, active el relé de la puerta para restringir el acceso cuando un evento involucre a un usuario en lista negra.

En la sección **Action**, haga clic en el interruptor **Relay** para habilitar la acción. Luego haga clic en el botón . Aparece

la ventana emergente de ajustes del relé.



- **Port**: Seleccione el puerto del relé para activar. Seleccione el puerto del relé en el dispositivo o en un subdispositivo conectado al dispositivo. Los puertos usados por otras reglas o puertas muestran "En uso" y el sistema impide seleccionarlos.
- **Open Time**: Defina cuánto tiempo el relé permanece abierto. Mueva el control deslizante o ingrese un valor en el campo de entrada. Configúrelo en 1–120 segundos.
  - **Keep until event off**: Configure **Type** como **People Counting** y especifique el área definida en **Count Limit** como condición para usar **Keep until event off**. Esta opción mantiene el relé abierto hasta que finaliza el evento de límite de conteo, sin importar el tiempo.



- **Contact Type**: Seleccione el tipo de contacto del relé. Seleccione un puerto de repetidor para establecer las opciones. El valor predeterminado es **Normal Close**.
  - **Normal Open**: Normalmente abierto y se cierra cuando se activa el relé.
  - **Normal Close**: Normalmente cerrado y se abre cuando se activa el relé.
- **Schedule**: Seleccione el horario en que la regla se ejecuta y activa el relé.

Haga clic en **Apply** para guardar los ajustes de operación del relé.

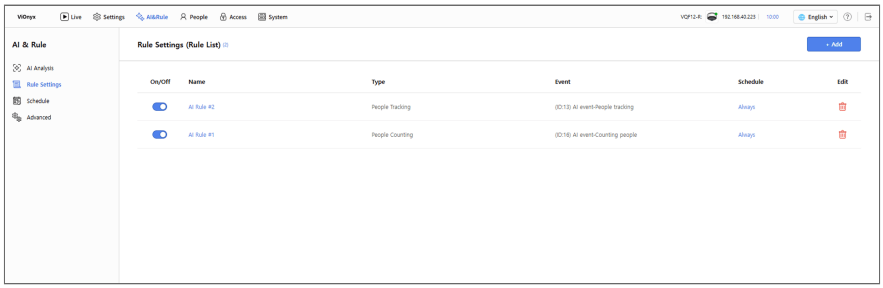
> **Precaución**
>
> **Contact Type** es un ajuste aplicado al puerto del relé, no una regla. El sistema aplica de inmediato el cambio de **Contact Type** a todas las reglas y puertas que usan el puerto. Cuando el puerto está fijo en Bloquear o Desbloquear, cambiar **Contact Type** invierte la salida y puede abrir una puerta bloqueada.

Información

- La versión de firmware 1.1.0 o posterior incluye soporte para esta característica.
- Cree, edite o elimine horarios en **AI&Rule** → **Schedule**. Para más información sobre la gestión de horarios, consulte Administrar horarios.

8 Guardar regla

Después de completar la configuración de la regla, haga clic en **Save** en la parte superior derecha para guardar la regla. Las reglas guardadas aparecen en la lista de reglas. La lista de reglas muestra el nombre de la regla, el tipo, el evento y el horario.



Habilitar/Deshabilitar reglas de IA

En la lista de reglas, haga clic en el interruptor de la izquierda de una regla para habilitarla o deshabilitarla. Las reglas habilitadas ejecutan las acciones configuradas cuando ocurre un evento de IA. Las reglas deshabilitadas no ejecutan acciones cuando ocurren eventos de IA.

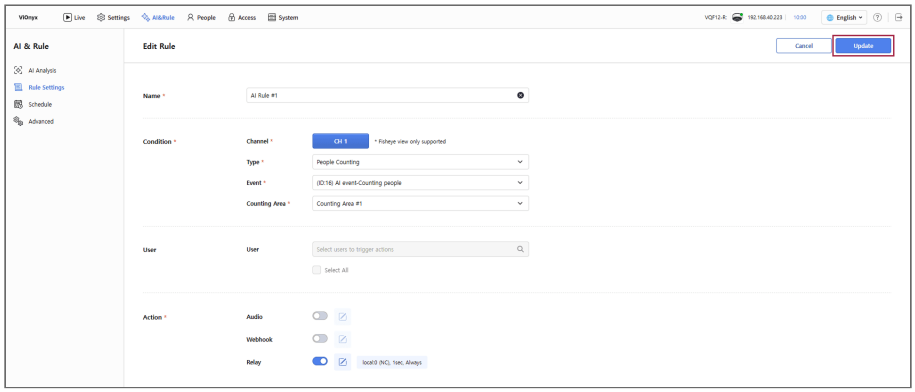


Información

La lista de reglas muestra el estado de habilitación de un vistazo. Las reglas con un interruptor azul están habilitadas; las reglas con un interruptor gris están deshabilitadas.

Editar regla de IA

Haga clic en una regla de la lista de reglas para ver o editar sus detalles. En la pantalla de detalles de la regla, después de modificar las condiciones y las acciones, haga clic en **Update** para guardar los cambios.



Eliminar regla de IA

En la lista de reglas, haga clic en a la derecha de una regla para eliminarla. Las reglas eliminadas no se pueden recuperar.



Administrar horarios

Un horario es un calendario semanal que combina días de la semana y franjas horarias. Cuando una acción de regla de IA usa un horario, la acción se ejecuta solo durante las franjas horarias del horario. Un solo horario se puede usar en varias reglas de IA.

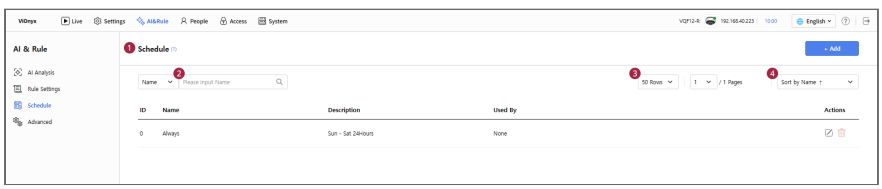
Crea horarios en las siguientes situaciones.

- Enviar webhooks solo durante el horario laboral de lunes a viernes
- Reproducir el audio de alerta de detección de intrusión solo por la noche
- Evitar que los relés operen los fines de semana

> **Información**
>
> El dispositivo ofrece el horario **Always** de forma predeterminada. El horario Always se ejecuta las 24 horas del día y no se puede editar ni eliminar.

Revisa la lista de horarios

1. Haga clic en el menú **AI&Rule** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Schedule** en la barra lateral izquierda.



La lista de horarios muestra los horarios registrados y las reglas de IA que usan cada horario.

- Junto a **Schedule**(1) en la parte superior de la pantalla, el sistema muestra la cantidad de horarios.
- Ingresa el nombre o el ID del horario en el campo de búsqueda (2) para encontrar un horario específico.
- Selecciona un valor de la lista Filas por página (3) para definir los horarios por página.
- Para cambiar el orden de clasificación, selecciona un criterio de la lista **Sort by Name**(4).

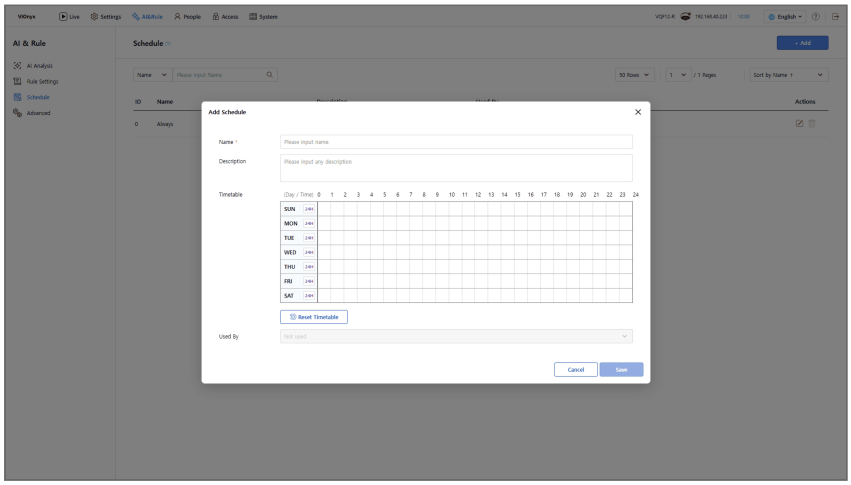
La lista de horarios muestra lo siguiente.

Ítem	Descripción
ID	Identificador único del horario. El horario Always es `0`.
Name	Nombre del horario.
Description	Descripción que se ingresa al agregar o editar el horario.
Used By	Reglas de IA que usan el horario. Si ninguna regla de IA usa el horario, aparece **None**. Si varias reglas de IA usan el horario, aparecen con el formato **and {count} more**.
Actions	Esta característica permite editar ( ) o eliminar ( ) horarios.

Agregar horario

1 Comienza a agregar un horario

1. Haz clic en **+ Add** en la parte superior derecha de la pantalla de lista de horarios.
2. Ingrese la información del horario cuando aparezca la ventana emergente **Add Schedule**.

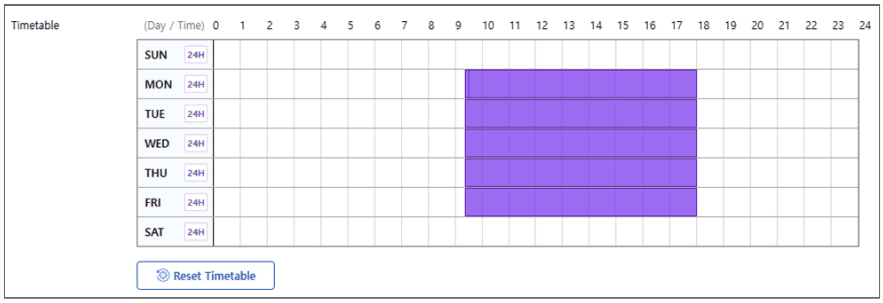


2 Ingrese un nombre y una descripción

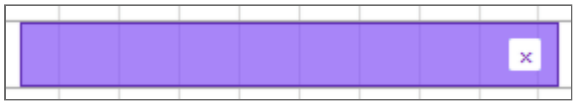
- **Name**: Introduzca el nombre del horario. Este campo es obligatorio. Use un nombre único para cada horario. Ingresa hasta 48 caracteres.
- **Description**: Ingrese una descripción para el horario. Por ejemplo, agregue un rango de tiempo aplicado como **Lun-Vie 09:00-18:00** para distinguir horarios al seleccionarlos en reglas.

3 Defina franjas horarias en la tabla horaria

Seleccione los días y las franjas horarias en las que se aplica el horario en **Timetable**. El eje vertical muestra el día de la semana (domingo~sábado) y el eje horizontal muestra la hora (0~24). Las franjas horarias seleccionadas aparecen como bloques.



- **Seleccionar franjas horarias**: Arrastre desde la hora de inicio hasta la hora de fin en la fila del día deseado. Seleccione en incrementos de 10 minutos.
- **Mover una franja horaria**: Arrastre el bloque a la izquierda o a la derecha para moverlo a otra hora.
- **Seleccionar o borrar 24 horas**: Haz clic en **24H** junto al nombre del día. La tabla horaria selecciona las 24 horas de ese día. Haz clic de nuevo para borrar todo.
- **Eliminar un bloque**: Seleccione el bloque para eliminarlo. Aparece el icono ✕. Haz clic en el botón Eliminar bloque.



- **Inicializar todo**: Para borrar todas las franjas horarias y definirlas de nuevo, haz clic en **Reset Timetable**.

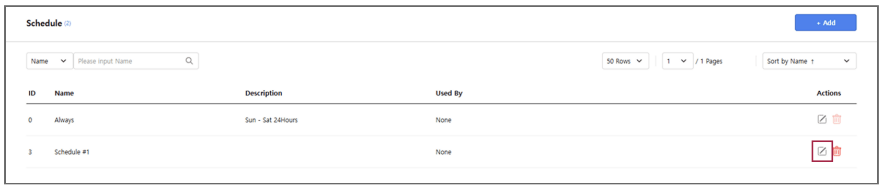
4 Guardar horario

Después de completar todos los ajustes, haga clic en **Save**. El sistema agrega el horario guardado a la lista de horarios. Selecciónelo en los ajustes de operación de reglas de IA.

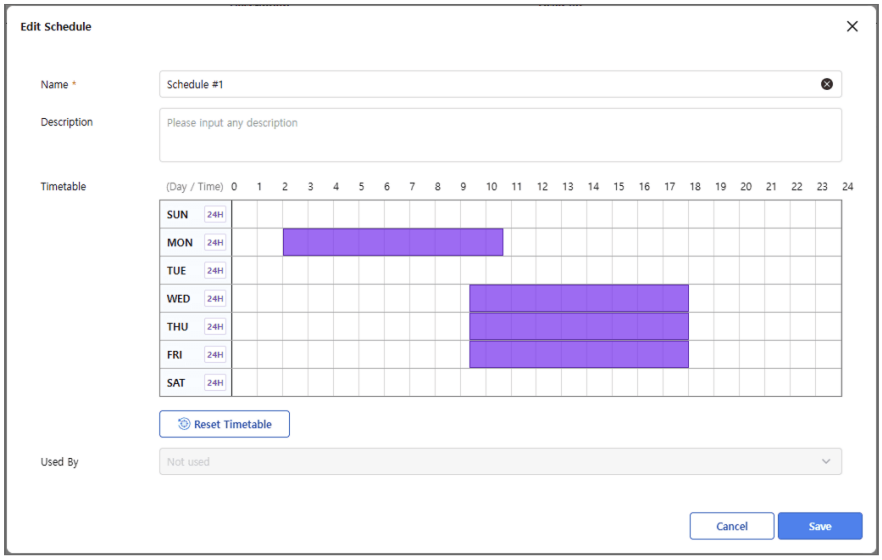
> **Información**
>
> - El campo **Used By** es de solo lectura y muestra las reglas de IA que usan el horario. Un horario recién creado aún no tiene reglas de IA que lo usen, por lo que aparece como **Not used**.
> - Para aplicar un horario guardado a una regla de IA, consulte Ajustes de Reglas de IA.

Modificar horario

1. En la lista de horarios, haga clic en el botón a la derecha del horario.



2. Cuando aparezca la ventana emergente **Edit Schedule**, edite el nombre, la descripción y la tabla horaria.



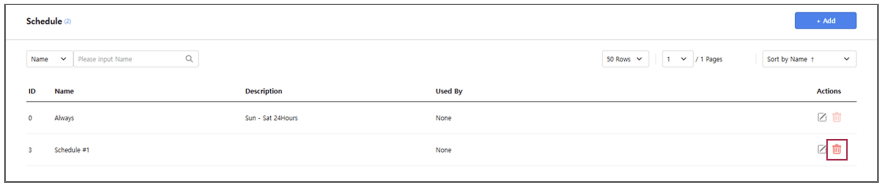
3. Haga clic en **Save** para guardar los cambios.

Al guardar el horario modificado, el sistema lo aplica a todas las reglas de IA que lo usan.

> **Información**
>
> - Si varias reglas de IA comparten un horario, revise las reglas afectadas en la columna **Used By** antes de editar.
> - El horario Always, el horario predeterminado, no se puede modificar.

Eliminar horario

1. En la lista de horarios, haga clic en el botón a la derecha del horario.



2. Si aparece un mensaje de confirmación, revíselo y haga clic en **OK**.

Los horarios eliminados no se pueden recuperar.

Información

- No elimine horarios que usan las reglas de IA. En las reglas de IA de la columna **Used By**, seleccione otro horario y luego intente eliminarlo de nuevo.
- El horario Always, el horario predeterminado, no se puede eliminar.

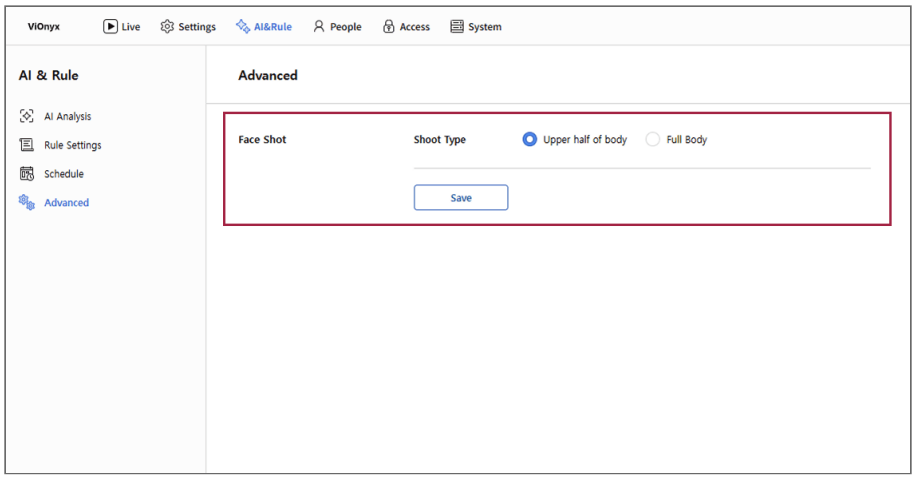
Configuración Avanzada

En la configuración avanzada, puedes establecer el tipo de captura de rostro y administrar las políticas automáticas de enrolamiento y retención de usuarios enrolados cuando ocurre el reconocimiento facial.

Configuración del tipo de captura de rostro

Establece el tipo de captura de rostro para capturar solo la parte superior del cuerpo o el cuerpo completo.

1. Haga clic en el menú **AI&Rule** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Advanced** en la barra lateral izquierda.
3. Selecciona el tipo de captura deseado en la opción **Shoot Type**, luego haz clic en **Save**.



Configuración de enrolamiento automático de usuarios

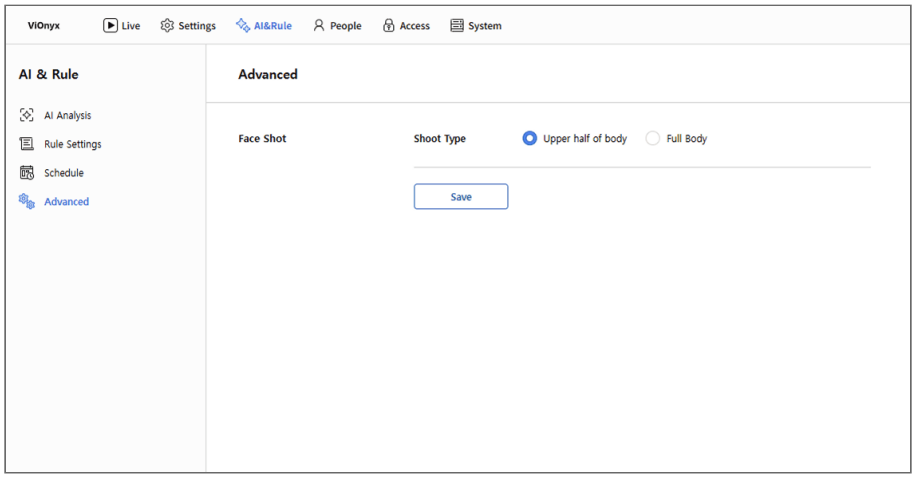
Los rostros detectados mediante eventos de IA se pueden enrolar automáticamente como usuarios. De forma predeterminada, esta función está en el modo Enrolamiento manual. Cambia al modo Enrolamiento automático según sea necesario.

Información

Para los usuarios enrolados automáticamente, edita manualmente información como el nombre de usuario y la descripción. Para obtener más información sobre cómo editar la información del usuario, consulta Editar y Eliminar Usuarios.

Habilitar el modo de enrolamiento automático

1. Haga clic en el menú **AI&Rule** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Advanced** en la barra lateral izquierda.
3. En la sección **Auto User Enroll**, haz clic en el interruptor para habilitar el modo de enrolamiento automático.



Configura cada opción como se indica a continuación y luego haz clic en **Save** para guardar.

> **Información**
> Cuando se usa el modo **Auto User Enroll**, los usuarios enrolados con fotos de baja calidad, como imágenes borrosas, rostros con mascarilla o de perfil, pueden experimentar autenticación incorrecta.

Configuración del número de usuarios para enrolamiento automático

En la opción **# of Auto Enroll User**, establece el número de usuarios que se pueden enrolar automáticamente. Arrastra el control deslizante o ingresa un número directamente en el campo de entrada.

- El valor predeterminado es 50,000 usuarios y admite hasta 100,000 usuarios.
- Al establecer el número de usuarios para enrolamiento automático, el total de enrolamientos automáticos y manuales no puede superar el límite configurado. Por ejemplo, si el número de usuarios configurado es 50,000, el total de enrolamientos automáticos y manuales solo puede llegar a 50,000 usuarios.

> **Información**
>
> - Si ya existen usuarios enrolados manualmente, no es posible aumentar el número de usuarios para enrolamiento automático.
> - Cuando disminuyes el número de usuarios para enrolamiento automático, el sistema elimina automáticamente a los usuarios excedentes, empezando por los más antiguos.

Configuración de la política de retención

En la opción **Retention Policy**, establece la política de retención para los usuarios enrolados automáticamente. Elige cómo eliminar a los usuarios enrolados automáticamente cuando se alcance el límite de usuarios.

- **Delete oldest when full**: Cuando se excede el número de usuarios asignado, elimina automáticamente primero a los

usuarios enrolados más antiguos.

Configuración del período de retención

En la opción **Retention Period (Days)**, establece en días el período de retención para los usuarios enrolados automáticamente. Cuando vence el período de retención, los usuarios enrolados más antiguos se eliminan automáticamente primero.

- **Disabled** (predeterminado): Cuando se excede el número de usuarios asignado, elimina automáticamente primero a los usuarios enrolados más antiguos.
- **1 day**, **3 days**, **7 days**, **14 days**, **30 days**, **90 days**, **365 days**: Elimina automáticamente a los usuarios enrolados automáticamente después de que termine el período seleccionado.

> **Información**
> Al establecer un período de retención, cuando se alcanza el límite de usuarios, el sistema elimina usuarios antiguos de inmediato; no espera a que termine.

Ver y administrar usuarios enrolados automáticamente

Ver en el menú **People**

Los usuarios enrolados automáticamente aparecen en la lista de usuarios del menú **People**.

- Los IDs de usuario se asignan automáticamente en secuencia según el orden de autenticación facial.
- La columna **Description** muestra **Auto Enroll**, lo que permite distinguir a estos usuarios de los usuarios enrolados manualmente.
- La columna **Last Updated** muestra la fecha y hora en que se enroló al usuario.

Editar detalles del usuario

1. Haga clic en el menú **People** en la esquina superior izquierda de la pantalla.
2. Haz clic en el usuario enrolado automáticamente de la lista de usuarios.
3. Cuando aparezca la ventana emergente de detalles del usuario, edita la información requerida.
4. Después de editar la información del usuario, haz clic en **Apply**.

Ver registros de autenticación facial y capturas de rostro

1. Haga clic en el menú **People** en la esquina superior izquierda de la pantalla.
2. Haz clic en el usuario enrolado automáticamente de la lista de usuarios.
3. Cuando aparezca la ventana emergente de detalles del usuario, consulta los registros de autenticación facial en la sección **Event Logs**.

- Selecciona una fecha para ver los registros de autenticación facial de un período específico.
- Haz clic en **Face Shot** en el registro para mostrar la foto del rostro de ese momento de autenticación.

Configurar la Cámara

Después de instalar la cámara, configúrela según el entorno de instalación y el uso previsto. Esta sección explica los ajustes de calidad de video, privacidad, hora, red e integración con dispositivos y sistemas externos. Seleccione los ajustes necesarios a continuación.

Configurar Perfil de Video

La calidad de la imagen de vista en vivo y la calidad del video grabado dependen de los ajustes del perfil de video. En los ajustes del perfil de video, ajuste los modos de vista por canal y los valores de codificación de transmisión. También ofrece las funciones de Espejo (inversión izquierda-derecha) y restablecimiento de canal según el entorno de instalación.

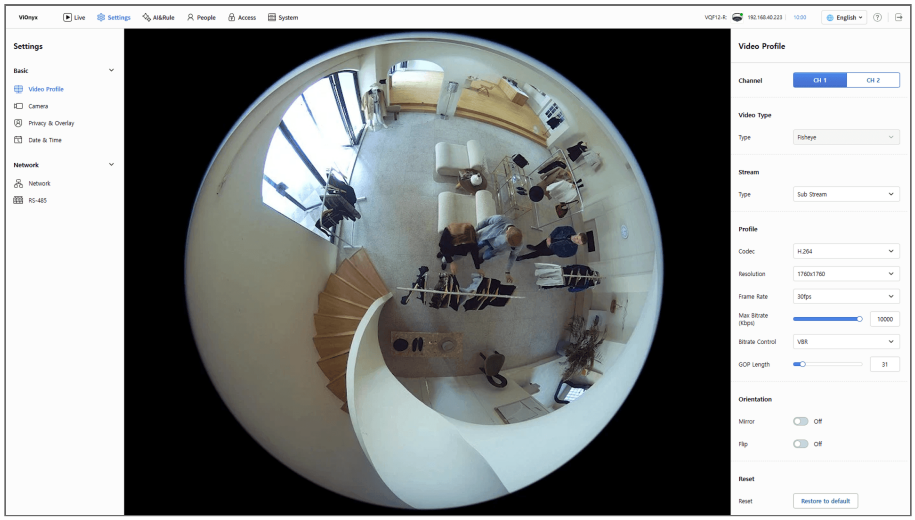
Configure el perfil de video en las siguientes situaciones para equilibrar la calidad de imagen, el almacenamiento y el ancho de banda de red.

- Cuando equilibra el almacenamiento y la calidad de imagen
- Cuando separa las transmisiones principal y secundaria para ajustarlas al ancho de banda de red
- Cuando usa modos de vista por canal para ajustarlos a su propósito previsto

> **Información**
>
> Si los eventos de IA están activos, cambiar el ajuste de espejo o realizar un restablecimiento puede eliminar los ajustes de eventos de IA.

Ajustes del perfil de video

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Basic** → **Video Profile** en la barra lateral izquierda.



> **Información**
> Los cambios del perfil de video se aplican a la cámara de inmediato sin un botón separado de guardar.

Selección de canal y tipo de vista

El propósito principal de cada canal es el siguiente.

- **CH 1**: Este canal funciona según la vista ojo de pez original de la cámara física.
- **CH 2**: Este canal usa vistas procesadas, como pantallas panorámicas o divididas en cuatro, para mejorar la eficiencia de monitoreo.

Defina los ajustes detallados del perfil de video por canal de cámara.

1. Desde el panel derecho **Video Profile**, seleccione **CH 1** o **CH 2** en **Channel**.
2. En **Video Type** → **Type**, seleccione el tipo de vista para el canal seleccionado.

Las políticas del tipo de vista por canal son las siguientes.

- **CH 1**: Fijo en ojo de pez y no se puede cambiar.
- **CH 2**: Seleccione un modo de vista distinto de ojo de pez.
  - **Single Panorama**: Este modo corrige el video capturado por una cámara ojo de pez para que pueda ver una vista panorámica tipo muro.
  - **Double Panorama**: Este modo corrige la distorsión en el video capturado de un área de 360° para que pueda ver una vista panorámica dividida en pantalla superior e inferior.
  - **Quad View**: Este modo corrige la distorsión según la visión humana y permite ver 4 pantallas específicas a la vez.

Selección del tipo de transmisión

En **Stream**, seleccione la transmisión que va a configurar. Seleccione la transmisión principal o secundaria y luego ajuste los valores detallados en la sección **Profile**.

- **Main Stream**: Grabación y monitoreo de alta calidad
- **Sub Stream**: Monitoreo remoto de bajo ancho de banda

> **Información**
> El canal **CH 2** solo admite **Main Stream**.

Ajustes detallados del perfil

Ajuste el códec, la resolución, la velocidad de fotogramas y otros ajustes detallados según el tipo de transmisión seleccionado.

- **Codec**: Seleccione el códec que se aplicará al perfil. Seleccione una de estas opciones: **H.264**, **H.265** o **MJPEG**.

> Seleccionar H.265 requiere Profile T.

- **Resolution**: Resolución que se aplicará al perfil. Las resoluciones admitidas varían según el canal, el tipo de video y el tipo de transmisión.

Canal	Tipo de video	Tipo de transmisión	Resolución admitida
CH 1	**Fisheye**	**Main Stream**	3520 × 3520
		Sub Stream	1760 × 1760
CH 2	**Single Panorama**	**Main Stream**	2048 × 512, 1920 × 480, 1280 × 320, 704 × 176
	Double Panorama	**Main Stream**	2048 × 2048, 1920 × 1920, 1280 × 1280, 704 × 704
	Quad View	**Main Stream**	2048 × 2048, 1600 × 1600, 1280 × 1280, 1024 × 1024

> El canal **CH 2** solo admite **Main Stream**.

- **Frame Rate**: Establezca la cantidad de fotogramas por segundo. Seleccione uno de estos valores: 30, 25, 20, 15 o 10 fotogramas por segundo.
- **Max Bitrate**: Establezca la tasa de bits de video máxima.
- **Bitrate Control**: Seleccione el método de control de la tasa de bits de video.
  - **VBR**: La tasa de bits variable se ajusta según la complejidad de la escena y ofrece alta calidad cuando la red es estable. Recomendado cuando el ancho de banda de red es suficiente.
  - **CBR**: La tasa de bits constante garantiza una transmisión estable, pero puede reducir la calidad en escenas complejas. Recomendado cuando el ancho de banda de red es limitado o constante.
- **GOP Length**: Establezca el intervalo de I-frame. Seleccione un valor entre 1 y 300. Un GOV más largo reduce el tamaño de los datos; uno más corto lo aumenta.

> **Información**
>
> - **Tasa de bits variable** (VBR): Este método transmite video dentro de la tasa de bits máxima sin fijar el tamaño de datos de cada fotograma. La tasa de bits varía según la complejidad de la escena. Por lo general ofrece alta calidad, pero puede causar interrupciones de video cuando el ancho de banda de red es inestable.
> - **Tasa de bits constante** (CBR): Este método transmite video fijando el tamaño de datos de cada fotograma. Ofrece una transmisión estable en entornos con ancho de banda de red constante, pero la calidad puede degradarse según la complejidad de la escena.
> - **GOV** (Group of Video): En la compresión H.264/H.265, esto se refiere al grupo de fotogramas desde un I-frame hasta el fotograma inmediatamente anterior al siguiente I-frame. Un GOV contiene I-frames (fotogramas clave) que conservan todos los datos de la imagen y P-frames que solo contienen los cambios respecto al fotograma anterior. Un GOV más largo reduce los fotogramas I y los datos de video. Un GOV más corto aumenta los fotogramas I y los datos de video.

Ajustes de espejo

Según la ubicación de instalación de la cámara, es posible que se requieran ajustes de espejo o de volteo.

- **Mirror**: Active o desactive el ajuste de espejo.
- **Flip**: Active o desactive el ajuste de volteo.

> **Información**
> Cambiar el espejo puede estar restringido cuando se configuran eventos de IA. Siga las instrucciones emergentes para eliminar los ajustes de IA y continuar.

Inicialización de ajustes del canal

Haz clic en **Restore to default** en **Reset** para restaurar el modo de vista y los ajustes de transmisión del canal seleccionado a los valores predeterminados de fábrica.

> **Información**
> - Solo el canal seleccionado se restaura a los valores predeterminados de fábrica.
> - Si se establece un evento de IA en modo ojo de pez, elimine el ajuste de IA antes de continuar.

Configurar Ajustes de la Cámara

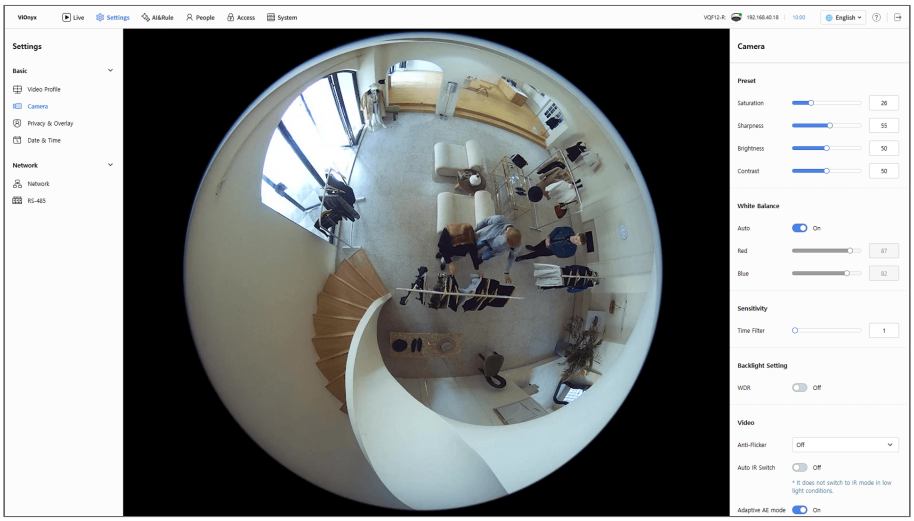
Ajuste los parámetros de la cámara para capturar video óptimo para el entorno de instalación. Los cambios aparecen de inmediato en Vista en vivo. Verifique los resultados mientras ajusta la calidad de imagen, el balance de blancos, la sensibilidad y la compensación de contraluz. Las características de IA disponibles varían según el tipo de montaje (techo o pared).

Ajuste los parámetros de la cámara en las siguientes situaciones.

- Para mejorar la calidad de imagen y adaptarla al brillo y color de la escena.
- Para minimizar el ruido en entornos con poca luz mientras mantiene la detección de movimiento.
- Cuando un contraluz intenso desde una ventana o puerta hace que el sujeto se vea oscuro
- Para reducir el parpadeo de la iluminación fluorescente o LED.
- Cuando hay iluminación complementaria o se requiere video a color, y el cambio a IR por la noche debe permanecer desactivado
- Cuando la luz ambiental hace que un rostro se vea muy oscuro o muy brillante, la autenticación facial puede ser difícil
- Para optimizar la cámara y las funciones de IA para la ubicación de instalación.
- Cuando se forme condensación o escarcha en el lente por el frío o la humedad y la imagen se vea borrosa

Ajustes de la cámara

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haga clic en **Basic** → **Camera** en la barra lateral izquierda.



> **Información**
> Cada cambio de opción aparece en Live View en tiempo real y se guarda automáticamente.

Ajustar calidad de imagen

Ajuste la calidad de imagen para adaptarla al entorno de captura. Ajuste cada control deslizante en la sección **Preset** para ver los cambios en la vista previa en tiempo real. Establezca valores entre 1 y 100.

- **Saturation**: Ajuste la saturación del color. (Predeterminado: 26)
- **Sharpness**: Ajuste la nitidez de la imagen. (Predeterminado: 55)
- **Brightness**: Ajuste el brillo general de la imagen. (Predeterminado: 50)
- **Contrast**: Ajuste el contraste entre las áreas claras y oscuras. (Predeterminado: 50)

> **Información**
> Al mover un control deslizante, cada ajuste actualiza la vista previa de inmediato y se guarda automáticamente.

Ajustes de balance de blancos

Configure el balance de blancos para que la cámara reproduzca con precisión el color de la iluminación de la escena. En la sección **White Balance**, active o desactive la opción **Auto**.

- **On**(predeterminado): La cámara detecta y ajusta automáticamente la temperatura de color.
- **Off**: Configure el balance de blancos ajustando manualmente los valores **Red** y **Blue**.

Ajustes de sensibilidad (Time Filter)

Ajuste el filtro de tiempo para equilibrar la reducción de ruido del sensor y la detección rápida de movimiento. Ajuste el control deslizante **Time Filter** en la sección **Sensitivity** para definir la intensidad del filtrado de ruido.

- Bajo (1~30): El filtrado de ruido débil ayuda a detectar objetos en rápido movimiento, pero el ruido puede aumentar en entornos con poca luz.
- Medio (31~70): Filtrado equilibrado, adecuado para entornos de captura típicos.
- Alto (71~100): El filtrado de ruido intenso reduce el ruido en condiciones de poca luz, pero puede dificultar la detección de objetos en rápido movimiento.

> **Información**
> El valor predeterminado de **Time Filter** es 1.

Ajustes de contraluz

Active WDR (Wide Dynamic Range) para que la cámara capture al mismo tiempo las áreas claras y oscuras en escenas a contraluz. En la sección **Backlight Setting**, active la opción **WDR** para activar la compensación de contraluz. (Predeterminado: **Off**)

> **Información**
> El modo **WDR** (Wide Dynamic Range) permite que la cámara ajuste la exposición automáticamente para representar tanto las áreas claras como las oscuras en escenas a contraluz. Activar WDR evita la sobreexposición de las áreas claras y mejora el detalle en las áreas oscuras. Útil al capturar en entornos con fuerte contraluz.

Ajustes de anti-parpadeo

Para reducir el parpadeo de la pantalla causado por una discrepancia entre la iluminación y la frecuencia, establezca la opción **Anti-Flicker** en la sección **Video**.

- **Off** (predeterminado): Desactive el anti-parpadeo.
- **50HZ**: entorno fluorescente/LED de 50 Hz
- **60HZ**: entorno fluorescente/LED de 60 Hz

> **Información**
> Seleccione la opción que coincida con la frecuencia de iluminación de la escena. Los ajustes incorrectos pueden causar parpadeo o bandas en la imagen.

Ajuste del cambio automático a IR

Defina si la cámara cambia automáticamente al modo IR (noche) cuando baja la luz ambiental. Desactive el cambio automático en áreas con iluminación complementaria o donde se requiera video a color. En la sección **Video**, active o desactive la opción **Auto IR Switch**.

- **On** (predeterminado): Cambia automáticamente al modo IR cuando baja la luz ambiental, según el sensor de iluminancia y el brillo de la imagen.
- **Off**: No cambia al modo IR en entornos con poca luz.

> **Información**
> La versión de firmware 1.1.0 o posterior admite la opción **Auto IR Switch**.

Ajuste del modo AE adaptativo

Cerca de una ventana o donde la luz solar cambia mucho, la autenticación facial puede ser difícil. Use el modo AE adaptativo en este caso. La cámara aprende dónde suelen aparecer los rostros y ajusta la exposición para que se vean bien iluminados. En la sección **Video**, active o desactive la opción **Adaptive AE mode**.

- **On** (predeterminado): Ajusta la exposición según el brillo del área del rostro.
  - Mantiene el brillo del área del rostro uniforme con luz ambiental intensa o cambios de luz solar.
  - El brillo de la imagen se mantiene estable sin importar el color de la ropa, si las personas pasan o se quedan.
  - Cuando la iluminación se enciende o se apaga, reajusta la exposición al nuevo brillo.
- **Off**: No usa la corrección del modo AE adaptativo. Cuando lo vuelva a habilitar, la corrección se ejecuta automáticamente.

> **Información**
> - **Adaptive AE mode** opera según el área del rostro en eventos de IA y el rango de detección de personas. Para ajustar el área, consulte Administrar Eventos de IA.
> - La versión de firmware 1.1.0 o posterior admite la opción **Adaptive AE mode**.

Ajustes de tipo de montaje

Configure **Mounting Type** según la ubicación de instalación de la cámara. Las funciones de IA compatibles dependen del tipo de montaje.

- **Ceiling** (predeterminado): Seleccione para instalación en techo. Todas las funciones de IA están disponibles.
- **Wall**: Seleccione para instalación en pared. Solo está disponible Facial Authentication AI; el seguimiento de objetos no es compatible.

> **Información**
> - **Al cambiar de techo a pared**, aparece una ventana de confirmación que indica que solo está disponible Facial Authentication y que la IA de seguimiento de objetos no está disponible. Revise el mensaje antes de continuar.
> - **Al cambiar de pared a techo**, el cambio se aplica de inmediato y todas las funciones de IA se activan automáticamente.

Ajuste del calefactor de la cámara

Las bajas temperaturas o la alta humedad pueden empañar o escarchar el lente, desenfocar la imagen y reducir la precisión del reconocimiento de IA. Active el calefactor de la cámara para mantener el lente despejado. En la sección **Heater**, active o desactive la opción **Heater**.

- **On**: El calefactor funciona. El calefactor se apaga automáticamente después de 30 minutos.
- **Off** (predeterminado): Detiene el calefactor.

> **Información**
>
> - Para evitar sobrecalentamiento y consumo innecesario, el calefactor funciona durante 30 minutos, se apaga automáticamente y la opción cambia a **Off**. Si el lente sigue empañado o con escarcha después de que el calefactor se apague, active la opción de nuevo.
> - Se incluye soporte para la opción **Heater** en el firmware 1.1.0 o posterior.

Restablecer ajustes de la cámara

Para restaurar todos los ajustes de la cámara a los valores predeterminados de fábrica, haga clic en **Restore to default** en la sección **Reset**.

Configurar Ajustes de Privacidad y Superposición

El ajuste Privacy & Overlay permite ocultar áreas sensibles o difuminar rostros automáticamente en el video de la cámara. También muestra la fecha, la hora y el nombre de la cámara en el video para indicar claramente el origen y la hora de grabación. Todos los ajustes surten efecto de inmediato en Live View.

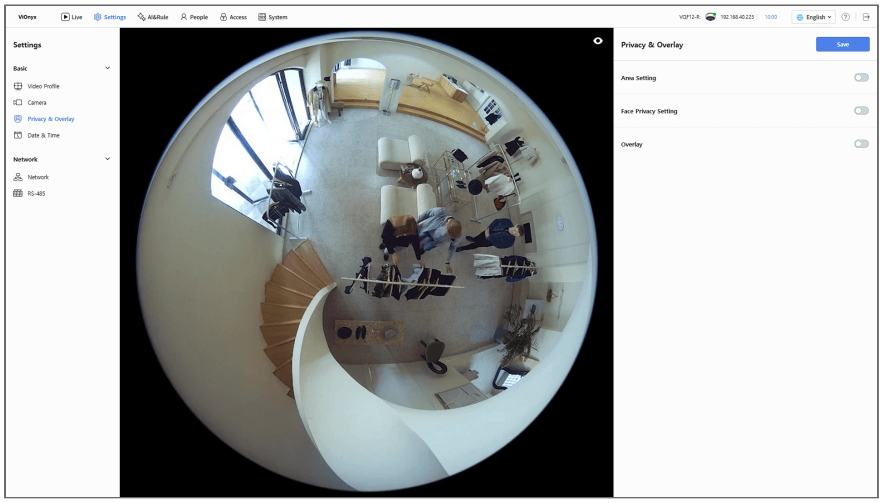
Configura Privacy & Overlay en las siguientes situaciones.

- Cuando necesitas ocultar áreas específicas que pueden invadir la privacidad
- Cuando necesitas cumplir con las políticas de privacidad al difuminar rostros automáticamente
- Cuando necesitas asegurar la trazabilidad del video grabado al mostrar la fecha y la hora
- Al operar varias cámaras, muestra los nombres de las cámaras para aclarar el origen del video

> **Información**
>
> Los ajustes de privacidad (ocultación, difuminado de rostros) solo se aplican a la visualización del video; el análisis de IA se ejecuta en las imágenes originales y no afecta el rendimiento de IA.

Ajustes de privacidad y superposición

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Basic** → **Privacy & Overlay** en la barra lateral izquierda.



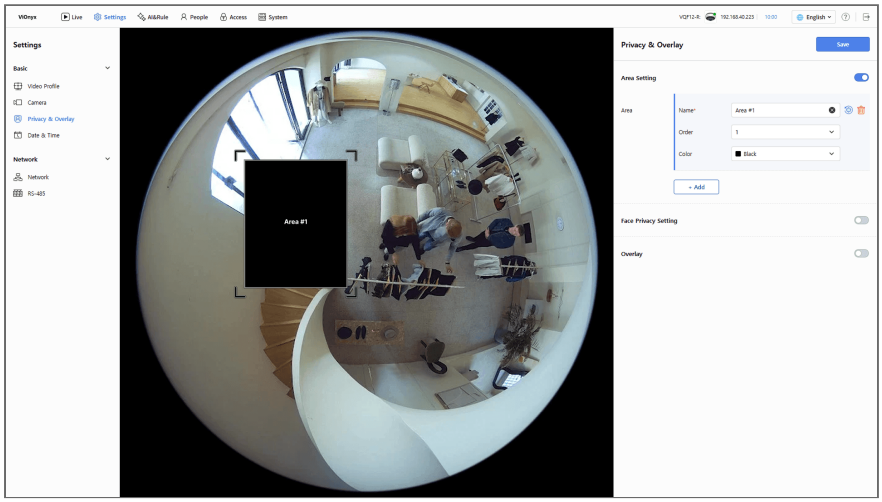
3. Para guardar los cambios, haz clic en **Save** en la esquina superior derecha de la pantalla.

Los cambios guardados se aplican a la cámara de inmediato después de guardar.

Ajustes del área de privacidad

Oculta áreas específicas en el video grabado que deben permanecer privadas. Configura hasta 10 áreas; cada área es fija y no se mueve.

1. Haz clic en el botón de alternancia en la sección **Area Setting**.
2. Haz clic en **+ Add**.
3. Se agrega un área de ocultación a Live View. Arrastra las esquinas del área para cambiar su tamaño, o arrastra toda el área para moverla.



4. Después de crear un área de ocultación, define el nombre, el orden y el color en el panel de ajustes derecho.
   - **Name**: El nombre del área de ocultación se genera automáticamente y se puede editar si es necesario.
   - **Order**: Ajusta el orden de visualización cuando las áreas de ocultación se superponen. Un número mayor aparece encima.
   - **Color**: Selecciona el color del área de ocultación.
5. Para guardar el área de ocultación agregada, haz clic en **Save** en la esquina superior derecha de la pantalla.

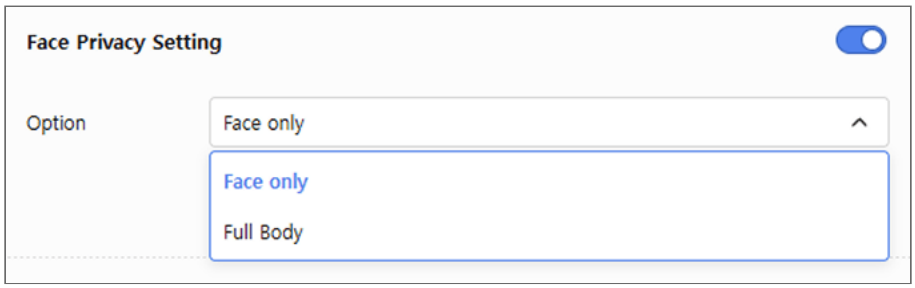
Las áreas de ocultación guardadas se aplican a Live View y al video grabado.

Información

- Las áreas ocultas se aplican automáticamente a todos los modos de visualización (ojo de pez, panorámica simple, panorámica doble y cuadrante).
- Para restablecer los ajustes del área de ocultación, haz clic en .
- Para eliminar un área de ocultación, haz clic en .

Ajustes de privacidad de rostros

Difumina automáticamente los rostros o cuerpos completos detectados para proteger la información personal. Activa **Face Privacy Setting** y elige el alcance de difuminado deseado.



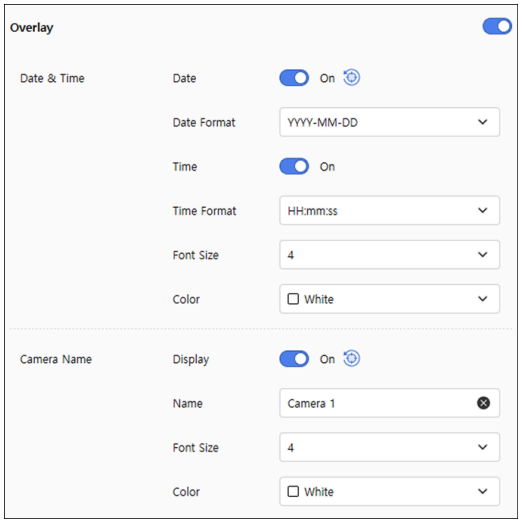
- **Face only**: Todos los rostros detectados se difuminan automáticamente.
- **Full Body**: Todo el cuerpo detectado se difumina automáticamente.

Información

Difuminar rostros o cuerpos completos no afecta el rendimiento de IA. Mientras la cámara muestra video difuminado, el análisis de IA se ejecuta en las imágenes originales, por lo que las funciones de IA, como Facial Authentication y el seguimiento de objetos, funcionan con normalidad.

Ajustes de superposición

Muestra la fecha, la hora y el nombre de la cámara en Live View. Activa **Overlay** y ajusta los detalles en **Date & Time** y **Camera Name**.





Información

Cada ajuste se guarda automáticamente al cambiarlo y se aplica de inmediato a Live View.

Date & Time

Define el formato, el tamaño y el color de la fecha y la hora que se muestran en Live View. En Live View, verifica la posición de la fecha y la hora, y arrástralas con el mouse para ajustar su posición o tamaño si es necesario.

- **Date** / **Time**: Haz clic en el botón de alternancia para activar o desactivar la superposición de la fecha y la hora.
- **Date Format**: Selecciona el formato de fecha.
  - AAAA-MM-DD (predeterminado, por ejemplo: 2026-01-12)
  - MM-DD-AAAA (por ejemplo: 01-12-2026)
  - DD-MM-AAAA (por ejemplo: 12-01-2026)
- **Time Format**: Selecciona el formato de hora.
  - HH:MM:SS (predeterminado, por ejemplo: 13:45:56)
  - HH:MM (se omiten los segundos, por ejemplo: 13:45)
- **Font Size**: Selecciona el tamaño de la fuente que se muestra en Live View. Selecciona un valor de 1 a 20.
- **Color**: Selecciona el color del texto que se muestra en Live View.

Información

La superposición de fecha y hora aparece solo en Fisheye View.

Camera Name

Muestra el nombre de la cámara en Live View para aclarar el origen del video. En Live View, verifica la posición del nombre de la cámara y arrástralo con el mouse para ajustar su posición o tamaño si es necesario.

- **Display**: Haz clic en el botón de alternancia para activar o desactivar la superposición del nombre de la cámara.

- **Name**: Ingresa el nombre de la cámara.
- **Font Size**: Selecciona el tamaño de la fuente que se muestra en Live View. Selecciona un valor de 1 a 20.
- **Color**: Selecciona el color del texto que se muestra en Live View.

Guardar ajustes

Verifica los ajustes de inmediato en Live View. Para guardarlos, haz clic en **Save** en la esquina superior derecha de la pantalla. Los ajustes guardados se aplican a la cámara y aparecen en Live View y en el video grabado.

Configurar Fecha y Hora

La configuración de fecha y hora mantiene exacto el reloj de la cámara. Seleccione una zona horaria y configure la hora manualmente o sincronícela automáticamente con un servidor NTP. La hora precisa garantiza la confiabilidad de las marcas de tiempo de video y de los registros de eventos de IA.

Revise la configuración de fecha y hora en las siguientes situaciones.

- Después de instalar la cámara, configure la zona horaria para que coincida con la región de operación.
- Para sincronizar el reloj de la cámara ingresando manualmente la hora exacta.
- Para mantener la hora precisa automáticamente durante períodos largos mediante un servidor NTP.
- Para unificar la hora en varias cámaras y simplificar el análisis y el seguimiento de video.

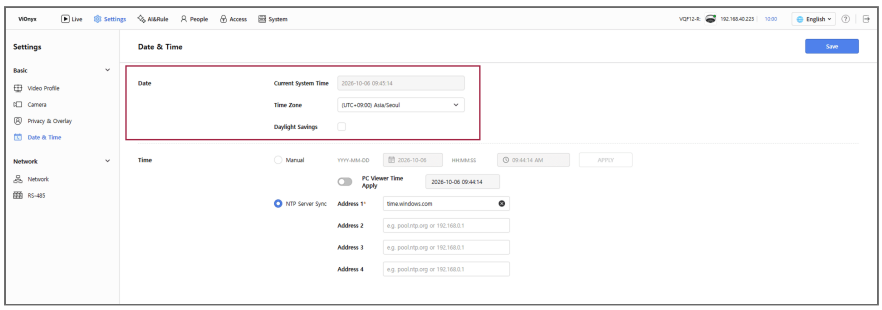
> **Información**
> La hora incorrecta de la cámara reduce la confiabilidad de los registros de eventos de IA, las marcas de tiempo de video y los registros del sistema. Revise la configuración de hora con regularidad.

Configuración de zona horaria

Primero, configure la zona horaria de la cámara para que coincida con la región de operación.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Basic** → **Date & Time** en la barra lateral izquierda.
3. En la sección **Date**, seleccione la región en **Time Zone**.

   Ejemplo: *(UTC+09:00) Asia/Seoul*



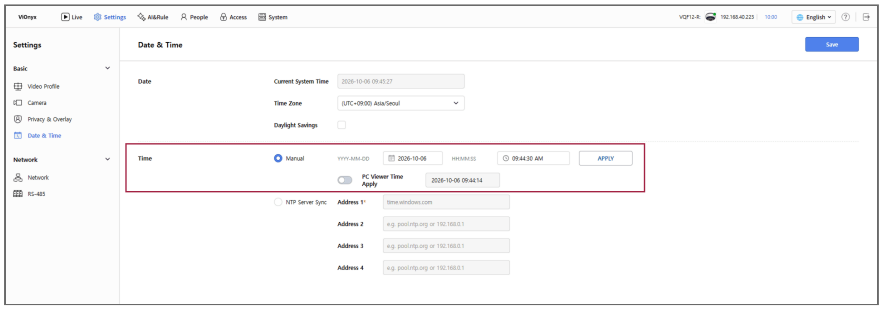
4. Para aplicar el horario de verano a la zona horaria, active la opción **Daylight Savings** marcando su casilla.
5. Haga clic en **Save** en la esquina superior derecha de la pantalla para guardar la zona horaria seleccionada.

> **Información**
>
> De forma predeterminada, se establece (UTC+09:00) Asia/Seoul. Si la región de operación es diferente, cambie la zona horaria.

Configuración manual de hora

Configure la hora de la cámara manualmente.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Basic** → **Date & Time** en la barra lateral izquierda.
3. En la sección **Time**, seleccione **Manual**.



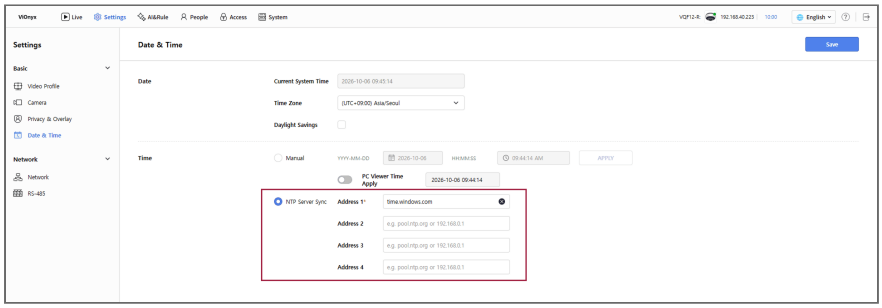
4. Ingrese la fecha actual en el campo Fecha, o haga clic en el icono de calendario para seleccionar una fecha.
5. Ingrese la hora actual en el campo Hora, o haga clic en el icono de reloj para seleccionar una hora.
6. Haga clic en **Apply** para aplicar la configuración de hora manual.
7. Haga clic en **Save** en la esquina superior derecha de la pantalla para guardar la configuración de hora.

> **Información**
>
> - Active la opción **PC Viewer Time Apply** para aplicar automáticamente la hora de la PC a la cámara. La hora del sistema en el navegador web se aplica a la cámara.
> - El modo manual y la sincronización automática NTP no pueden estar activos al mismo tiempo. Al seleccionar el modo manual, se desactiva la sincronización automática NTP.

Sincronización automática de hora

Use un servidor NTP para mantener automáticamente precisa la hora de la cámara. Recomendado para operación a largo plazo.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Basic** → **Date & Time** en la barra lateral izquierda.
3. En la sección **Time**, seleccione **NTP Server Sync**.



4. Ingrese la dirección del servidor NTP en el campo **Address {n}** (obligatorio).
   - Formato de URL: time.windows.com, time.nist.gov, etc.
   - Dirección IP: 192.0.2.1, etc.
5. (Opcional) Ingrese servidores NTP adicionales en **Address {n}**, **Address {n}** y **Address {n}** si es necesario.
   - Se admiten hasta 4 servidores.
   - Si **Address {n}** no responde, el sistema cambia automáticamente al siguiente servidor.
6. Haga clic en **Save** en la esquina superior derecha de la pantalla para guardar la configuración de hora.

Después de la configuración, la cámara se sincroniza automáticamente con el servidor NTP y actualiza la hora periódicamente.

> **Información**
>
> **Servidores NTP recomendados**
>
> - time.windows.com (NTP público de Windows)
> - time.nist.gov (NTP público de NIST)
> - pool.ntp.org (proyecto NTP Pool)

Configurar Ajustes de Red

Los ajustes de red establecen la dirección IPv4, la subred, la puerta de enlace y los servidores DNS del dispositivo. Establecen los puertos para la interfaz web y la transmisión de video en vivo. Seleccione asignación automática (DHCP) o manual (Static) según su entorno de red.

Configure el perfil que el NVR/VMS usa para conectarse mediante ONVIF. Conéctese al servicio externo en la nube Suprema CLUe para sincronizar la información de usuarios. Cloudflare Tunnel permite acceder a la interfaz web desde fuera de la red.

Revise los ajustes de red en las siguientes situaciones.

- Cuando la red admite DHCP y necesita que el dispositivo obtenga una dirección IP automáticamente.
- Cuando necesita acceso estable a la red mediante una dirección IP fija.
- Cuando los puertos predeterminados entran en conflicto con otros dispositivos o necesita cambiar los puertos por seguridad.
- Cuando conecta mediante ONVIF a un NVR/VMS heredado que no admite Profile T

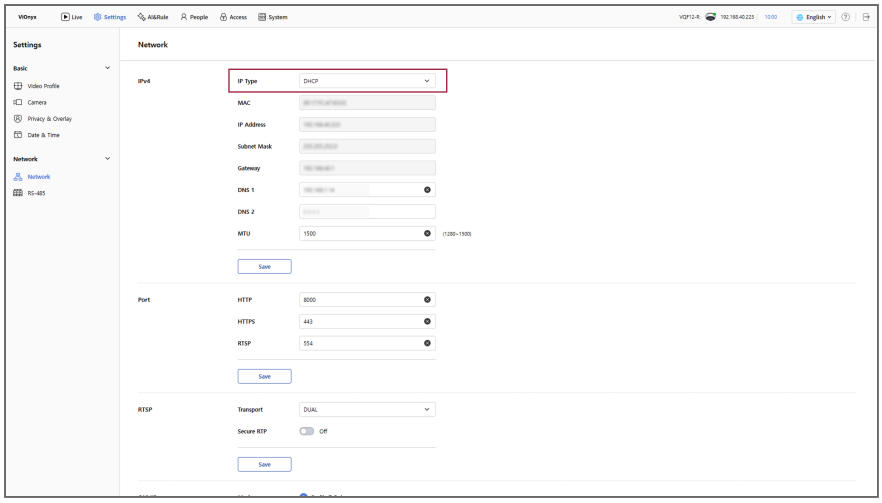
- Cuando sincroniza la información de usuarios con el servicio en la nube Suprema CLUe
- Cuando accede a la interfaz web del dispositivo desde fuera de la red sin reenvío de puertos ni una dirección IP pública

> **Información**
> Cambiar los ajustes de red, especialmente la dirección IP, puede desconectar las conexiones activas. Vuelva a conectarse usando la nueva dirección IP.

Dirección IP automática

DHCP asigna direcciones IP automáticamente en la red. En la mayoría de los entornos de red habituales, se configura automáticamente sin ajustes adicionales.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haga clic en **Network** → **Network** en la barra lateral izquierda.
3. Seleccione **DHCP** en **IP Type**.



4. Si necesita direcciones de servidor **DNS**, escríbalas en los campos de entrada **DNS {n}** y **DNS {n}**.
5. Ajuste el valor de **MTU** (Unidad Máxima de Transmisión) en el campo de entrada **MTU** según sea necesario.
   - El valor predeterminado es 1500.
   - Establezca un valor entre 1280 y 1500.
6. Haga clic en **Save** para guardar los ajustes de red.

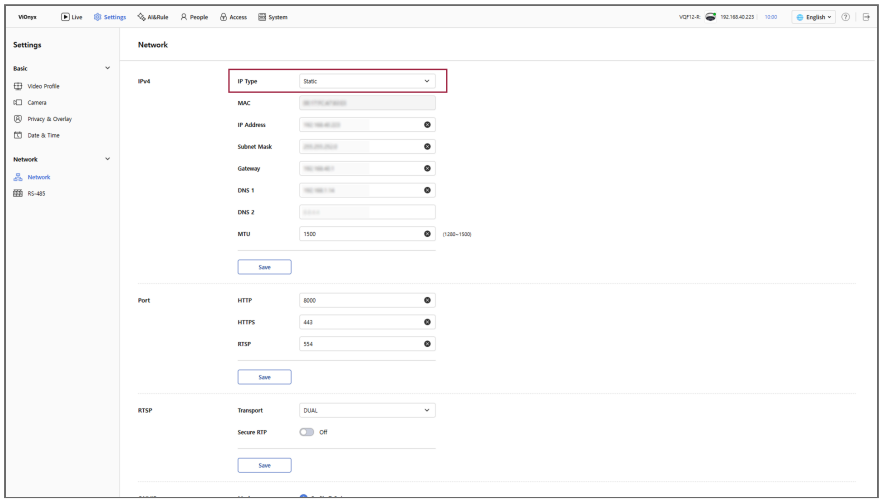
Si los ajustes se guardan correctamente, la dirección IP asignada aparece en los campos de entrada **IP Address**, **Subnet Mask** y **Gateway**.

> **Información**
> El modo DHCP está configurado de forma predeterminada y funciona automáticamente en la mayoría de los entornos de red estándar sin ajustes adicionales.

Dirección IP estática

Establezca la dirección IP manualmente cuando la red requiera una IP fija para un acceso estable.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haga clic en **Network** → **Network** en la barra lateral izquierda.
3. Seleccione **Static** en **IP Type**.



4. Escriba la dirección IPv4 asignada en el campo de entrada **IP Address**.

   > *Ejemplo: 192.168.111.11*

5. Escriba la máscara de subred en el campo de entrada **Subnet Mask**.

   > *Ejemplo: 255.255.255.0*

6. Escriba la dirección de la puerta de enlace en el campo de entrada **Gateway**.
7. Escriba la dirección del servidor DNS en los campos de entrada **DNS {n}** y **DNS {n}**.
8. Ajuste el valor en el campo de entrada **MTU** según sea necesario.
   - El valor predeterminado es 1500.
   - Establezca un valor entre 1280 y 1500.
9. Haga clic en **Save** para guardar los ajustes de red.

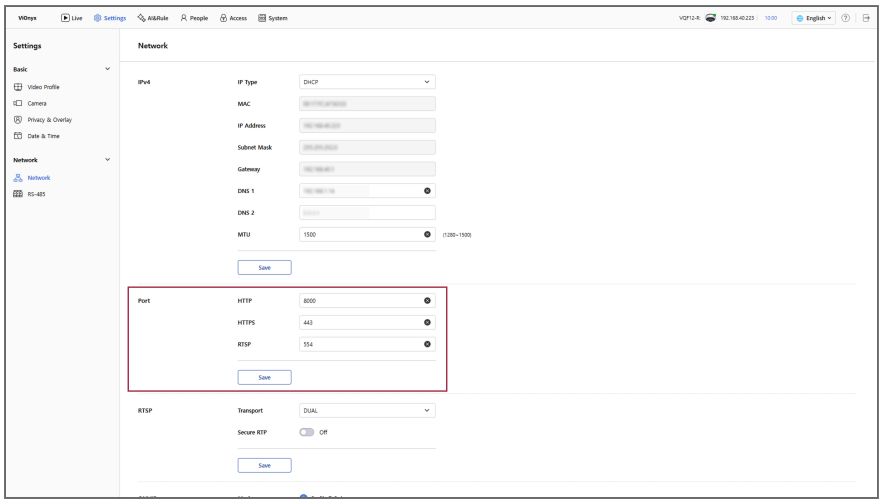
> Si no escribe una dirección válida en cada campo de entrada, aparece un borde rojo alrededor del campo y **Save** se desactiva. Después de escribir correctamente todos los campos de entrada, inténtelo de nuevo.

Ajustes de puertos

En la sección **Port**, establezca los números de puerto usados para acceder a la interfaz web (HTTP, HTTPS) y para la transmisión de video (RTSP).

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haga clic en **Network** → **Network** en la barra lateral izquierda.

3. Establezca los puertos necesarios en la sección **Port**.



- **HTTP**: Puerto para acceso sin cifrar a la interfaz web (predeterminado: 8000)
- **HTTPS**: Puerto para acceso cifrado a la interfaz web (predeterminado: 443)
- **RTSP**: Puerto para transmitir video mediante el protocolo RTSP (predeterminado: 554)

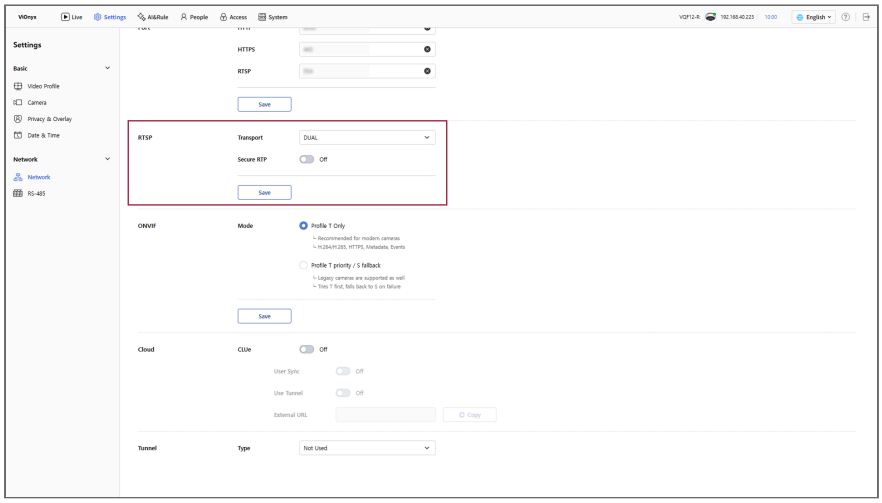
4. Haga clic en **Save** para guardar los ajustes de puertos.

> **Información**
>
> - Escriba un número del 1 al 65535 en cada campo de entrada de puerto.
> - No asigne el mismo número de puerto a varios servicios. Cada puerto debe tener un número único.
> - Si un puerto difiere del valor predeterminado, incluya el número de puerto en la URL de la interfaz web.
>
> > *Ejemplo: Si el puerto HTTPS es 4000:* `https://{ip_address}:4000`

Ajustes de transmisión y cifrado de video

En la sección **RTSP**, configure los ajustes de transmisión y cifrado de video.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haga clic en **Network** → **Network** en la barra lateral izquierda.
3. Establezca las siguientes opciones en la sección **RTSP**.



- **Transport**: Seleccione el protocolo de transporte usado para la transmisión de video.
  - **UDP**: Permite una transmisión más rápida, pero el video puede entrecortarse según las condiciones de la red.
  - **TCP**: Proporciona transmisión estable, pero puede haber latencia en comparación con **UDP** según las condiciones de la red.
  - **DUAL**: Selecciona automáticamente UDP o TCP para la transmisión según las condiciones de la red. Esta es la opción predeterminada recomendada para entornos generales.
  - **TLS**: Envía el flujo RTSP con cifrado TLS. Mejora la seguridad, pero puede aumentar la carga de la CPU. Comprueba si el NVR/VMS conectado admite TLS.
- **Secure RTP**: Active la opción de cifrado del flujo RTSP.

4. Haga clic en **Save** para guardar los ajustes.

Información

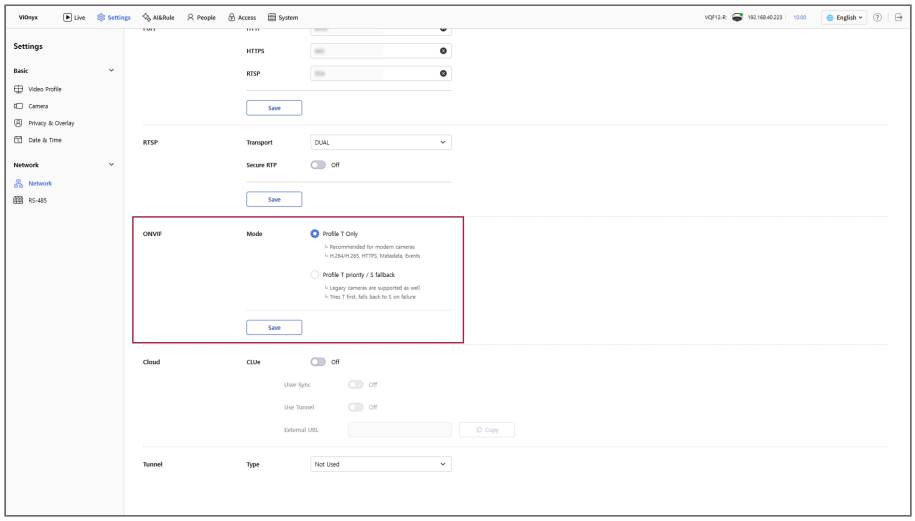
Si necesitas cifrado para los datos de video y audio, activa la opción **Secure RTP**, y comprueba si es compatible con el NVR/VMS conectado.

Precaución

Después de cambiar la opción **Secure RTP**, es posible que debas volver a conectar la sesión RTSP existente. Configura el NVR/VMS para que sea compatible con el método de transporte seleccionado.

Ajustes de ONVIF

En la sección **ONVIF**, configure el perfil que el NVR/VMS usa para conectarse mediante ONVIF. De forma predeterminada, el dispositivo usa solo Profile T. Habilite la alternativa a Profile S al conectar a un NVR/VMS heredado que no admite Profile T.



Seleccione uno de los dos modos siguientes.

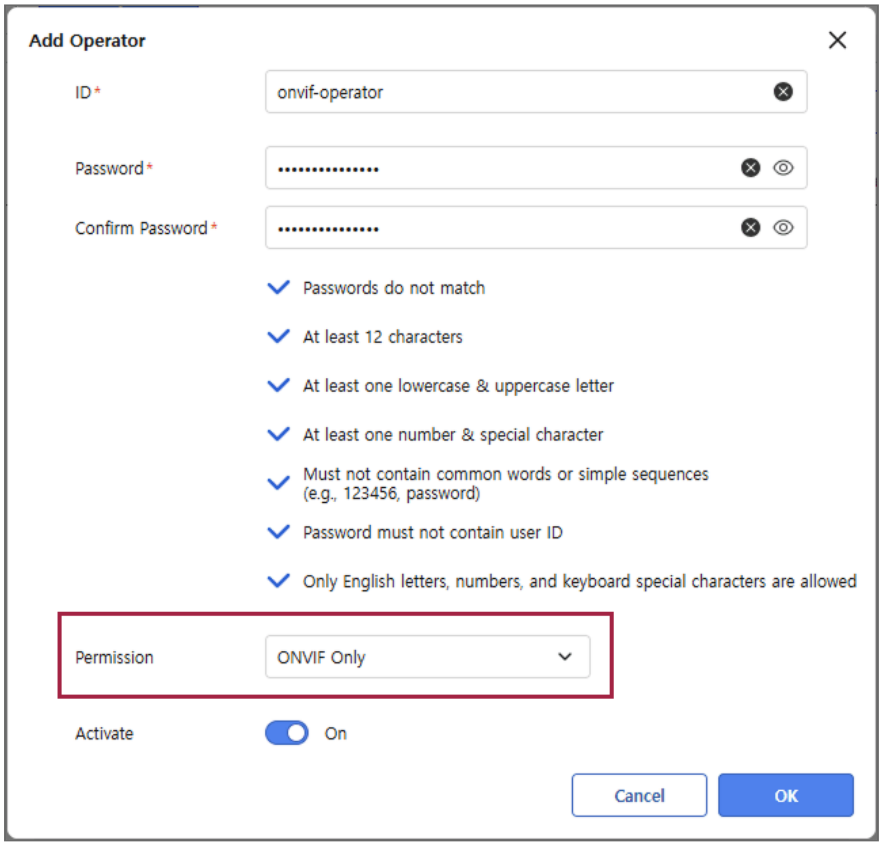
- **Profile T Only**: Conéctese solo con Profile T (Media2). Este modo admite los códecs H.264/H.265, HTTPS, metadatos y eventos, y se recomienda como valor predeterminado para entornos NVR/VMS modernos.
- **Profile T priority / S fallback**: El NVR/VMS primero intenta conectarse con el Perfil T y, si no es compatible, se conecta con el Perfil S (Media1). El NVR/VMS compatible con el Perfil T se conecta con el Perfil T en este modo.

Ítem	Profile T (Media2)	Profile S (Media1)
Códec	H.264, H.265	H.264, MJPEG
Comunicación cifrada	Compatibilidad con HTTPS	No compatible (comunicación en texto sin formato)
Funciones Avanzadas	Metadatos, eventos	Transmisión básica de video
Entorno recomendado	NVR/VMS más recientes	NVR/VMS antiguos que no admiten el Perfil T

Crea una cuenta solo para ONVIF

Crea una cuenta solo para ONVIF para autenticar ONVIF y RTSP antes de habilitar el respaldo del Perfil S. Si guardas los ajustes sin una cuenta, aparece el mensaje **Enabling the Profile S fallback requires an ONVIF-only account** y el sistema no guarda los ajustes.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Account** en la barra lateral izquierda.
3. En la sección **Operator**, haga clic en **+ Add**.
4. En la ventana emergente **Add Operator**, ingresa el nombre de usuario y la contraseña, y selecciona **ONVIF Only** en **Permission**.

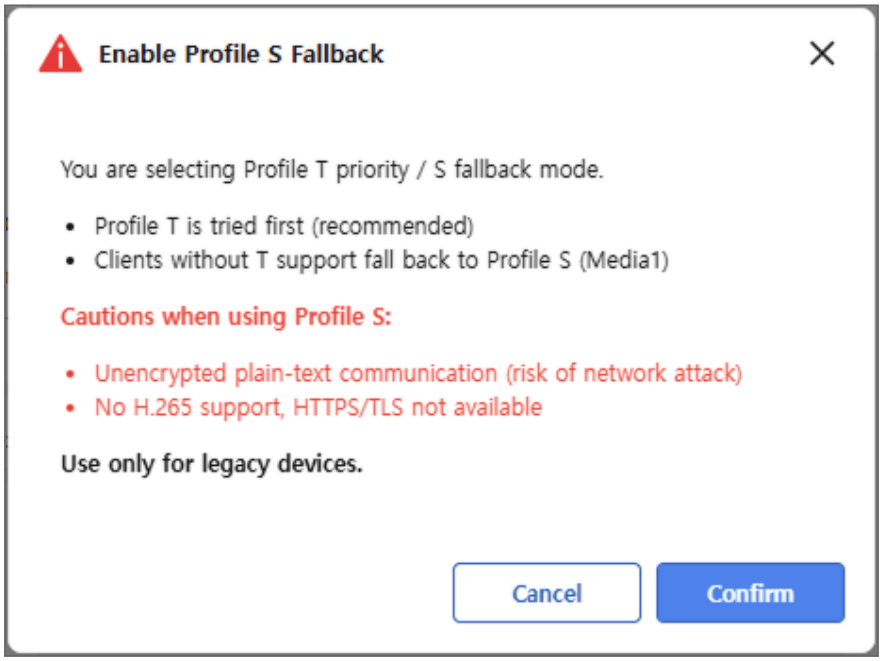


5. Haz clic en el botón **OK** para crear una cuenta solo para ONVIF.

Habilitar el respaldo del Perfil S

Habilita el respaldo del Perfil S.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haga clic en **Network** → **Network** en la barra lateral izquierda.
3. En la sección **ONVIF**, selecciona **Profile T priority / S fallback** en **Mode**.
4. Cuando aparezca la ventana emergente **Enable Profile S Fallback**, revisa las precauciones del Perfil S y haz clic en el botón **Confirm**.



5. Haga clic en **Save** para guardar los ajustes.

Cuando el sistema guarde los ajustes correctamente, aparece un mensaje de éxito en la esquina superior derecha de la pantalla. Al agregar el dispositivo al NVR/VMS, ingresa el ID y la contraseña de la cuenta solo para ONVIF.

Para deshabilitar el respaldo del Perfil S, selecciona **Profile T Only** y haz clic en el botón **Save**.

> **Precaución**
> El Perfil S envía tráfico sin cifrar en texto sin formato, lo que lo expone a ataques de red. Profile S tampoco admite el códec H.265 ni HTTPS/TLS. Úsalo solo al conectarte a NVR/VMS antiguos que no admiten Profile T.

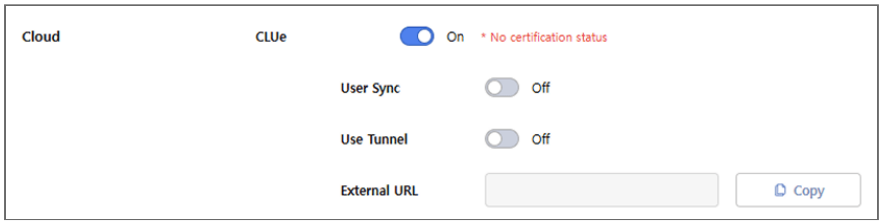
> **Información**
> - Solo los administradores pueden cambiar los ajustes de ONVIF.
> - Cada dispositivo permite solo una cuenta exclusiva de ONVIF. La cuenta no puede iniciar sesión en la IU web. El sistema no permite cambiar el ID ni la contraseña después de crear la cuenta.
> - Solo estas acciones están disponibles para la cuenta solo de ONVIF: habilitar, deshabilitar o eliminar. Si la cuenta está deshabilitada, el sistema no puede habilitar la conmutación por error de Profile S.
> - Para eliminar la cuenta solo de ONVIF, primero cambia a **Profile T Only**.
> - Los ajustes de ONVIF actualizados se aplican a las conexiones nuevas. Los flujos conectados mantienen el método actual hasta reconectarse.

Conexión en la nube CLUe

Suprema CLUe es un servicio de control de acceso basado en la nube. Conéctate a CLUe para sincronizar la información de usuarios con el servicio en la nube de CLUe.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haga clic en **Network** → **Network** en la barra lateral izquierda.

3. Haga clic en el interruptor **CLUe** de la sección **Cloud** para activarlo.
4. El sistema verifica la conexión a Internet y la conexión al servidor CLUe. El estado de conexión aparece a la derecha del interruptor **CLUe**.



   - *** Connecting...**: Conectando al servidor de CLUe.
   - *** Connected**: Conectado al servidor de CLUe.
   - *** Connection failed**: No se pudo conectar al servidor de CLUe. Revise la conexión a Internet e inténtelo de nuevo.
   - *** No certification status**: El dispositivo no está certificado por CLUe.
5. Habilita las opciones requeridas. Habilita el interruptor **CLUe** para usar las siguientes opciones.
   - **User Sync**: Sincroniza la información de usuarios con el servicio en la nube de CLUe.
   - **Use Tunnel**: Usa un túnel para el acceso externo al dispositivo mediante CLUe. Cuando el túnel se conecta, la URL aparece en el campo **External URL**. Haz clic en el botón **Copy** para copiar la URL.

> **Información**
>
> - Si la conexión es exitosa, aparece el mensaje **CLUe has been enabled**.
> - Si falla la conexión, aparece el mensaje **CLUe has been disabled**. Revise la conexión a Internet e inténtelo de nuevo.
> - Desactive el interruptor **CLUe** para desconectarse del servidor CLUe. **User Sync** y **Use Tunnel** dejan de estar disponibles. Sin embargo, el servidor CLUe conserva la información de enrolamiento.
> - Los éxitos y fallos de conexión a CLUe se registran en el registro del sistema.

Ajustes de túnel

En la sección **Tunnel**, use Cloudflare Tunnel para crear una URL externa y acceder a la interfaz web por Internet. Use esta opción cuando necesite acceso remoto sin reenvío de puertos del router ni una dirección IP pública.

En **Tunnel** > **Type**, seleccione una de las siguientes opciones.

Tipo	Descripción	Información requerida
Not Used	No use el túnel. Este es el valor predeterminado.	Ninguno
Cloudflare Tunnel (Quick)	Obtenga una URL externa temporal sin una cuenta de Cloudflare. La URL cambia cuando el dispositivo se reinicia.	Ninguno
Cloudflare Tunnel (Named)	Cree un túnel con un token de API de Cloudflare y use una URL externa fija con su dominio.	Cuenta de Cloudflare, dominio

Tipo	Descripción	Información requerida
Cloudflare Tunnel (Named, Token)	Conéctese a un túnel creado en el panel de Cloudflare con un token de conector.	Cuenta de Cloudflare, dominio, token de conector

Consejo

Use **Cloudflare Tunnel (Quick)** para pruebas o acceso remoto temporal. Use **Cloudflare Tunnel (Named)** o **Cloudflare Tunnel (Named, Token)** para acceso continuo con una dirección fija.

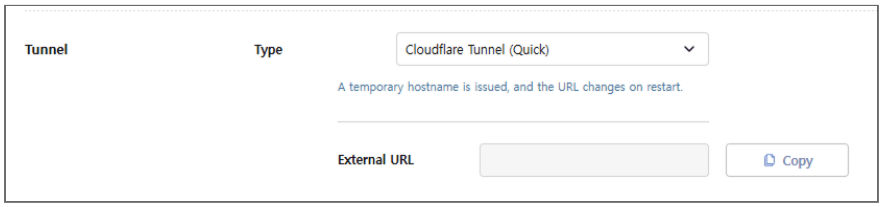
Información

- Para desactivar el túnel, seleccione **Not Used** en **Type**.
- Para usar el túnel, conecte el dispositivo a Internet.
- Cualquier persona que conozca la URL externa puede acceder a la página de inicio de sesión del dispositivo. Use contraseñas seguras para las cuentas de administrador y operador, y comparta la URL externa solo con usuarios autorizados.
- El registro del sistema guarda los cambios del modo de túnel.

Usar una URL externa temporal

Acceda al dispositivo mediante una URL externa temporal sin una cuenta de Cloudflare.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haga clic en **Network** → **Network** en la barra lateral izquierda.
3. En la sección **Tunnel**, seleccione **Cloudflare Tunnel (Quick)** en **Type**.



4. Cuando el sistema emite una URL externa temporal, aparece en el campo **External URL**. Haga clic en el botón **Copy** para copiar la URL y, luego, ábrala en un navegador web.

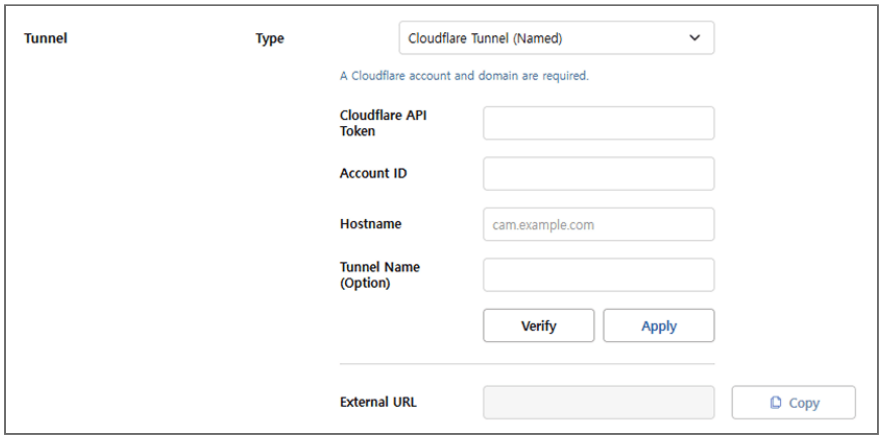
Precaución

La URL externa emitida con **Cloudflare Tunnel (Quick)** cambia cuando el dispositivo se reinicia. Después de reiniciar, verifique la nueva URL en el campo **External URL**.

Usar una URL externa fija (token de API)

Introduzca un token de API de Cloudflare. El dispositivo crea un túnel en Cloudflare y vincula la URL externa al nombre de host. Antes de comenzar, prepare una cuenta de Cloudflare y un dominio registrado en Cloudflare.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haga clic en **Network** → **Network** en la barra lateral izquierda.
3. En la sección **Tunnel**, seleccione **Cloudflare Tunnel (Named)** en **Type**.



4. Introduzca la siguiente información.
   - **Cloudflare API Token**: Introduzca el token de API emitido en el panel de Cloudflare.
   - **Account ID**: Introduzca el ID de cuenta de Cloudflare.
   - **Hostname**: Introduzca el nombre de host para el acceso externo.

     > *Ejemplo: cam.example.com*

   - **Tunnel Name (Option)**: Introduzca un nombre para identificar el túnel en Cloudflare. Opcional.
5. Haga clic en **Verify** para verificar la información introducida.
6. Haga clic en **Apply** para aplicar los ajustes.

Cuando el túnel se conecta, la URL externa aparece en el campo **External URL**. Haga clic en **Copy** para copiar la URL.

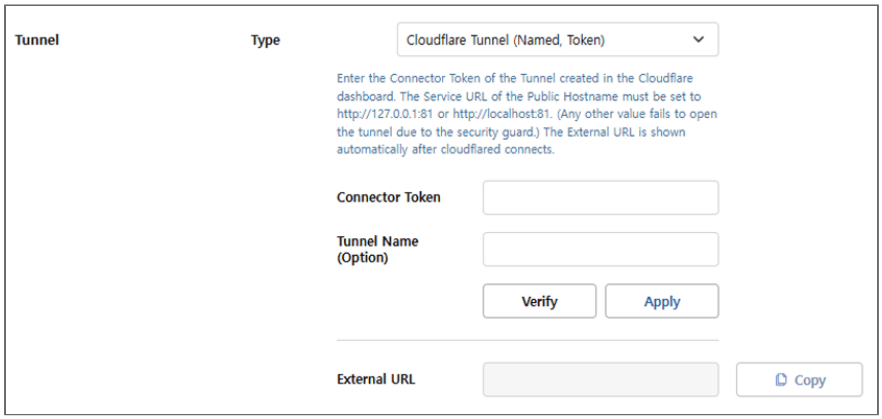
Usar una URL externa fija (token del conector)

Esta opción conecta el dispositivo a un túnel creado en el panel de Cloudflare. Antes de comenzar, completa las siguientes tareas en el panel de Cloudflare.

- Crea un túnel y copia el token del conector.
- Agrega el nombre de host público del túnel y establece la URL del servicio en `http://127.0.0.1:81` o `http://localhost:81`.

Después de completar los ajustes, sigue estos pasos en el dispositivo.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haga clic en **Network** → **Network** en la barra lateral izquierda.
3. En la sección **Tunnel**, en **Type**, selecciona **Cloudflare Tunnel (Named, Token)**.



4. Introduzca la siguiente información.
   - **Connector Token**: Introduce el token del conector copiado del panel de Cloudflare.
   - **Tunnel Name (Option)**: Introduce un nombre para identificar el túnel. Opcional.
5. Haga clic en **Verify** para verificar la información introducida.
6. Haga clic en **Apply** para aplicar los ajustes.

Cuando cloudflared se conecta, la URL externa aparece automáticamente en el campo **External URL**.

> **Precaución**
> Las políticas de seguridad evitan que el túnel se abra si la URL del servicio del nombre de host público no es `http://127.0.0.1:81` o `http://localhost:81`.

Configurar RS-485

En los ajustes de RS-485, agregue y administre dispositivos de E/S de Suprema conectados al puerto RS-485 de la cámara como esclavos. La cámara actúa como maestro del puerto RS-485. Vincule los relés del dispositivo esclavo registrado a reglas de IA para controlar dispositivos externos, como abrir puertas o encender luces de emergencia.

Revise los ajustes de **RS-485** en las siguientes situaciones.

- Al agregar un dispositivo de E/S a la cámara para aumentar las salidas de relé o los puertos de entrada
- Cuando ocurre un evento de IA y necesita controlar dispositivos externos mediante el relé de un dispositivo esclavo
- Al revisar el estado de conexión del dispositivo esclavo o actualizar el firmware
- Al eliminar un dispositivo esclavo que ya no se usa

Información

- La versión de firmware 1.1.0 solo admite el modo maestro. La cámara no admite el modo esclavo para conectarse a otro dispositivo como esclavo.
- Agregue hasta 8 dispositivos esclavos.
- Los dispositivos de E/S de Suprema son los únicos dispositivos esclavos compatibles. Los dispositivos de autenticación de huella digital y los dispositivos de autenticación facial no pueden conectarse como dispositivos esclavos.
  - Secure I/O 2 (SIO2)
  - Door Module (DM-20)
  - Door Interface (DI-24)
  - Output Module (OM-120)
  - Input Module (IM-120)

Antes de comenzar

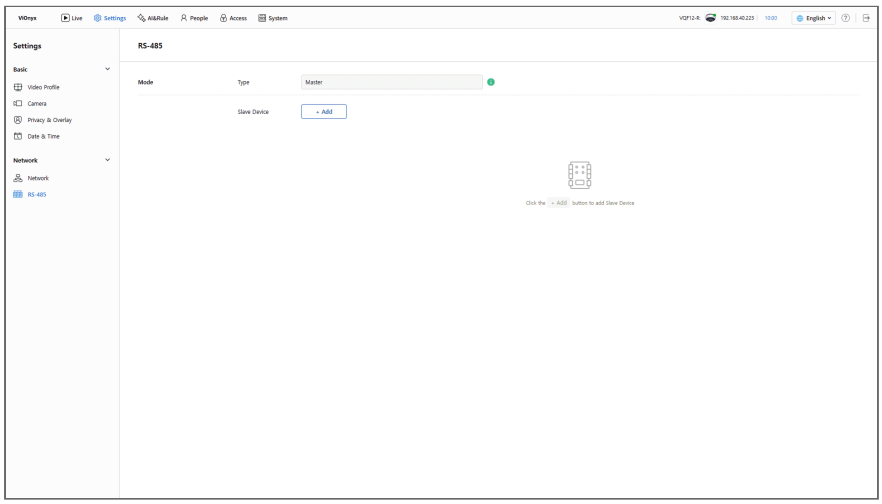
Revise lo siguiente antes de agregar dispositivos esclavos.

- Confirme que el dispositivo esclavo esté conectado correctamente al puerto RS-485 de la cámara.
- Confirme que el dispositivo esclavo tenga asignado un ID de OSDP. Los dispositivos con un ID de OSDP de 0 (sin asignar) no se pueden agregar.
- Confirme que los dispositivos en el mismo bus RS-485 tengan IDs de OSDP únicos.
- Si agregó el dispositivo esclavo a otro dispositivo maestro, inicialice el dispositivo.

Agregar dispositivos esclavos

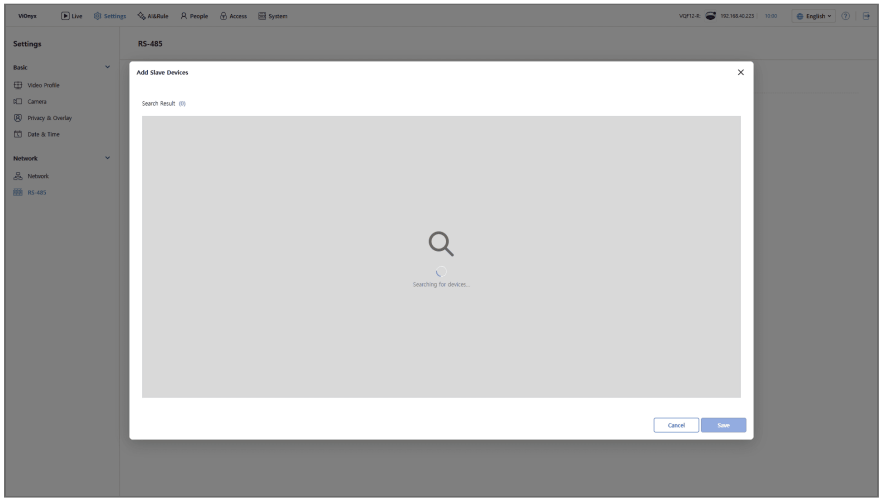
Busque dispositivos esclavos conectados al puerto RS-485 y agréguelos a la cámara.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Network** → **RS-485** en la barra lateral izquierda.

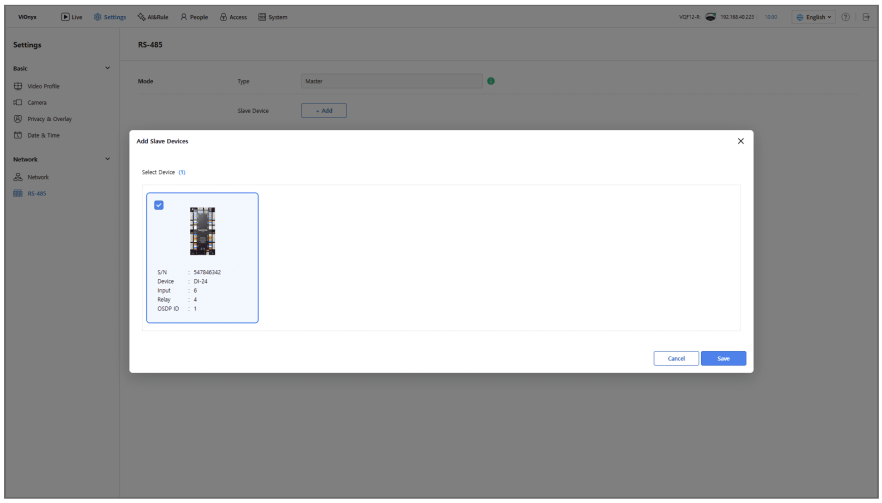


3. En **Slave Device**, haz clic en **+ Add**.

4. Aparece la ventana emergente **Add Slave Devices** y la búsqueda de dispositivos inicia automáticamente. Espere a que finalice la búsqueda.



5. Seleccione la casilla de verificación del dispositivo que agregará en los resultados de búsqueda. Seleccione varios dispositivos.



Los dispositivos detectados incluyen la siguiente información.

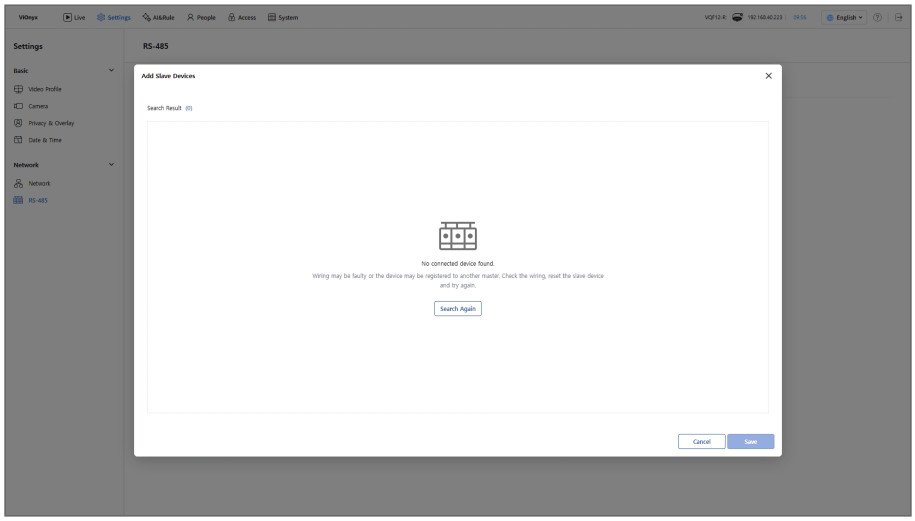
- **S/N**: Número de serie del dispositivo
- **Device**: Modelo del dispositivo
- **Input**: Número de puertos de entrada
- **Relay**: Número de puertos de relé
- **OSDP ID**: ID de OSDP asignado al dispositivo

6. Haga clic en **Save** para agregar el dispositivo seleccionado. Seleccione al menos un dispositivo para habilitar el botón.

Cuando el sistema agrega el dispositivo correctamente, aparece un mensaje de éxito en la esquina superior derecha. La lista **Slave Device** muestra los dispositivos en orden de ID de OSDP. De forma predeterminada, el nombre del dispositivo es el número de serie. Cámbielo en Editar dispositivo esclavo.

Cuando no se encuentran dispositivos

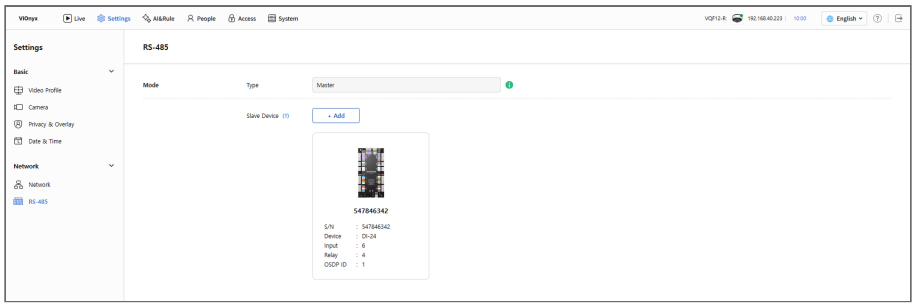
Si aparece el mensaje **No connected device found.** en los resultados de búsqueda, revise lo siguiente y luego haga clic en **Search Again**.



- Verifique que el cableado RS-485 del dispositivo esclavo esté conectado correctamente.
- Si el dispositivo esclavo está agregado a otro dispositivo maestro, inicialícelo.
- Confirme que el dispositivo esclavo tenga asignado un ID de OSDP.

Verificar el estado del dispositivo esclavo

Verifique la información del dispositivo y el estado de conexión en la lista **Slave Device**.



Cuando se desconecta la comunicación entre el dispositivo y la cámara, la tarjeta del dispositivo muestra **Disconnected** y la hora de desconexión. Verifique la alimentación del dispositivo y el cableado RS-485. El indicador desaparece cuando el dispositivo se reconecta.



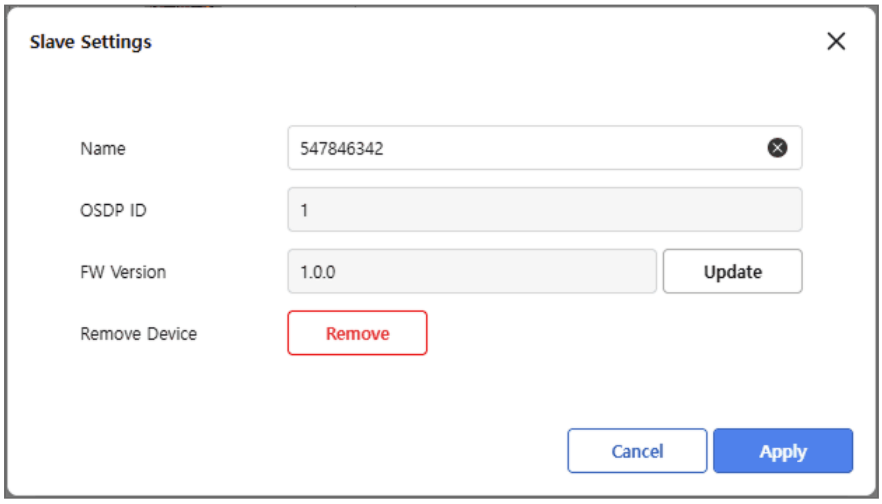
Información

Compruebe los registros de conexión y desconexión del dispositivo esclavo en el registro del sistema. Consulte Ver registros del sistema para obtener más información.

Editar dispositivo esclavo

Cambie el nombre de un dispositivo esclavo agregado.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Network** → **RS-485** en la barra lateral izquierda.
3. Pase el cursor sobre la tarjeta del dispositivo para editar y luego haga clic en el botón en la esquina superior derecha.
4. En la ventana emergente **Slave Settings**, introduzca un nombre nuevo en el campo **Name**.



5. Haga clic en **Apply** para guardar los cambios.

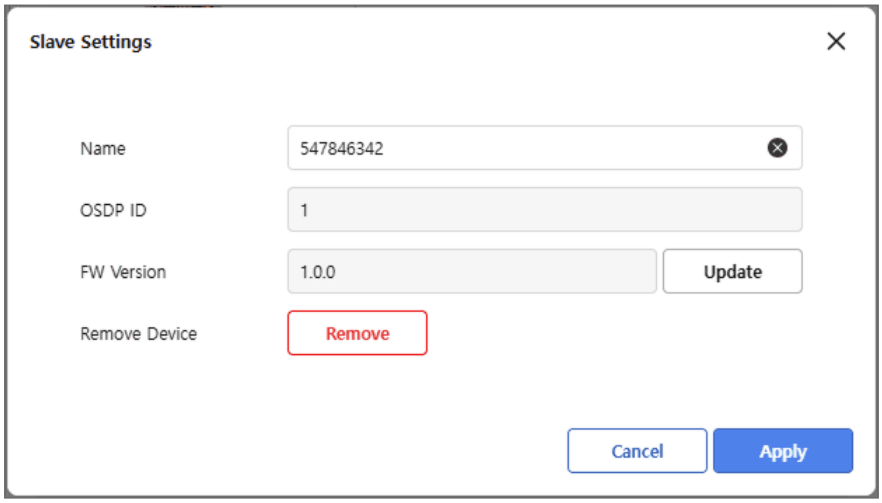
Cuando el sistema guarda los cambios correctamente, aparece un mensaje de éxito en la esquina superior derecha de la pantalla.

> **Información**
> En la ventana emergente **Slave Settings**, vea solo el ID de OSDP. No lo cambie.

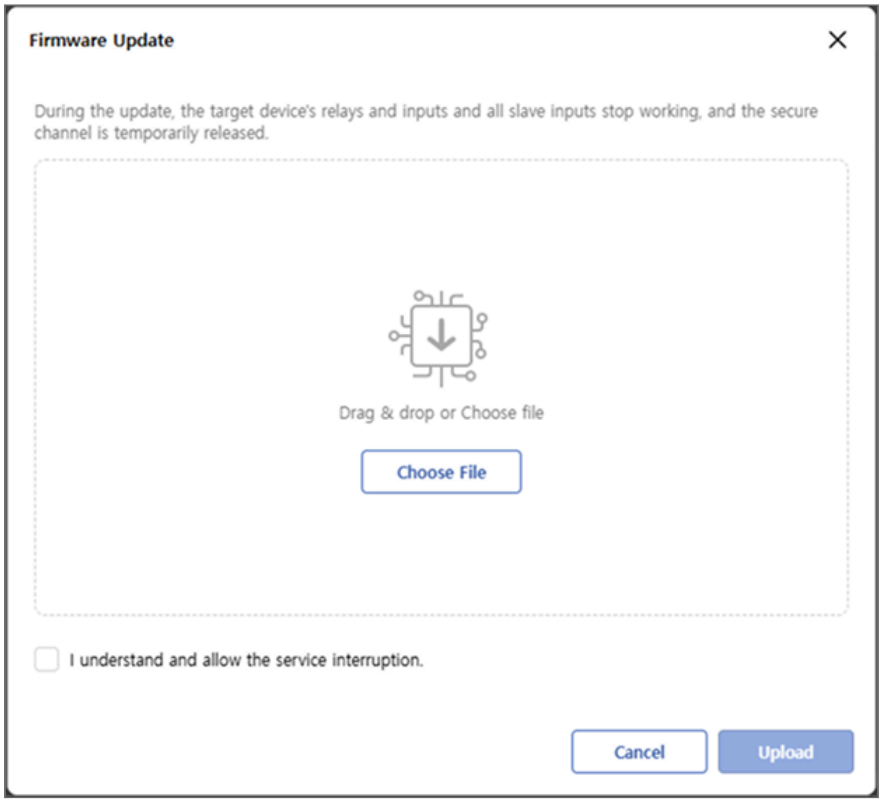
Actualizar firmware del dispositivo esclavo

En la ventana emergente **Slave Settings**, compruebe la versión actual del firmware y actualice el dispositivo esclavo.

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Network** → **RS-485** en la barra lateral izquierda.
3. Pase el cursor sobre la tarjeta del dispositivo para actualizar y luego haga clic en el botón en la esquina superior derecha.
4. En la ventana emergente **Slave Settings**, compruebe la versión actual en **FW Version** y luego haga clic en el botón **Update**.



5. Arrastre y suelte el archivo de firmware, o haga clic en **Choose File** para seleccionar un archivo.



6. Revise el aviso de interrupción del servicio y seleccione la casilla **I understand and allow the service interruption.**.
7. Haga clic en **Upload** para iniciar la actualización.

El estado y el progreso aparecen durante la actualización. Consulte el registro del sistema para ver registros de actualizaciones de firmware del dispositivo esclavo exitosas y fallidas.

Precaución

- La actualización interrumpe el relé y las entradas del dispositivo de destino, interrumpe las entradas de los dispositivos esclavos y deshabilita temporalmente el canal seguro. Ejecute la actualización cuando el dispositivo no esté en uso.
- No apague el dispositivo ni desconecte el cableado RS-485 durante la actualización.
- El sistema bloquea la actualización mientras otra actualización de firmware está en curso. Inténtelo de nuevo cuando finalice la actualización actual.

Eliminar dispositivo esclavo

Elimine los dispositivos esclavos que ya no se usan. Elimine los dispositivos de uno en uno o seleccione varios para eliminarlos a la vez.

Precaución

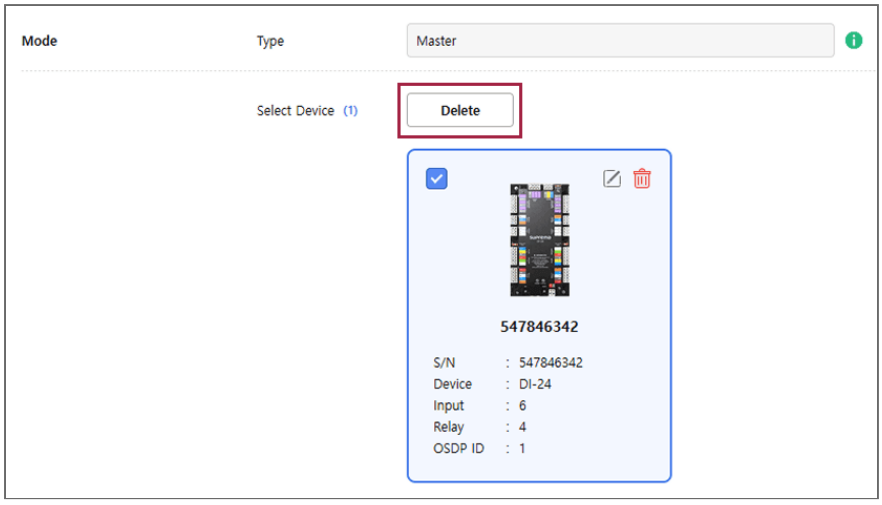
No se pueden eliminar los dispositivos usados en reglas de IA. Cuando intente eliminar un dispositivo, aparece el nombre de la regla que lo usa. Primero, quite de la regla el ajuste de relé del dispositivo y vuelva a intentarlo. Para editar reglas, consulte Ajustes de Reglas de IA.

Eliminar dispositivos uno por uno

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Network** → **RS-485** en la barra lateral izquierda.
3. Coloque el cursor sobre la tarjeta del dispositivo para eliminar y haga clic en el botón en la esquina superior derecha.
   - Como alternativa, haga clic en el botón y luego haga clic en **Remove** en la ventana emergente **Slave Settings**.
4. Cuando aparezca la ventana emergente **Remove Device**, haga clic en **Apply**.

Eliminar varios dispositivos a la vez

1. Haga clic en **Settings** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Network** → **RS-485** en la barra lateral izquierda.
3. Seleccione la casilla en cada tarjeta del dispositivo para eliminar. La cantidad de dispositivos seleccionados aparece junto a **Select Device**.



4. Haz clic en **Delete**.
5. Cuando aparezca la ventana emergente **Remove Device**, haga clic en **Apply**.

Cuando la eliminación se completa correctamente, aparece un mensaje de éxito en la esquina superior derecha de la pantalla.

Solución de Problemas

Pueden aparecer los siguientes mensajes de error al agregar, editar o eliminar un dispositivo esclavo.

Mensaje	Causa y solución
Failed to register the slave device. Check the wiring and try again.	El sistema no pudo comunicarse con el dispositivo. Revise el cableado RS-485 y vuelva a intentarlo.

Mensaje	Causa y solución
Up to 8 slave devices can be registered.	El sistema ya agregó 8 dispositivos. Elimine los dispositivos sin uso y luego agregue el dispositivo de nuevo.
A device with the same serial number is already registered.	Ya hay un dispositivo con el mismo número de serie en la lista. Revise la lista.
OSDP ID is already in use.	Otro dispositivo usa el mismo ID de OSDP. Cambie el ID de OSDP en el dispositivo esclavo y vuelva a buscar.
The OSDP ID collides with another device on the bus.	El ID de OSDP entra en conflicto con el de otro dispositivo en el bus RS-485. Cambie el ID de OSDP en el dispositivo esclavo y vuelva a buscar.
OSDP ID 0 (unassigned) cannot be registered. Assign an address on the device and search again.	Este dispositivo tiene un ID de OSDP de 0 (sin asignar). Asigne un ID de OSDP al dispositivo y vuelva a buscar.
Device search timed out.	El dispositivo no respondió antes de que se agotara el tiempo de espera de búsqueda. Revise el cableado y vuelva a buscar.
Slave device is in use by a rule.	Una regla de IA usa el dispositivo. Quite el ajuste de relé del dispositivo de la regla y vuelva a intentarlo.
RS-485 is initializing. Please wait.	La cámara está inicializando el puerto RS-485. Vuelva a intentarlo en un momento.

Integrar RTSP y ONVIF

La cámara admite transmisión RTSP (Real-Time Streaming Protocol) y el protocolo ONVIF (Open Network Video Interface Forum) para la integración estándar con NVR (Network Video Recorder) y VMS (Video Management Software) de terceros.

Consulta esta guía en los siguientes casos:

- Cuando quieres obtener video de la cámara mediante RTSP en un NVR/VMS de terceros
- Cuando quieres integrar la cámara con un NVR/VMS que admite ONVIF
- Cuando quieres consultar la información de la cuenta necesaria para una URL de acceso RTSP o la integración ONVIF

Transmisión RTSP

Puerto y método de transporte

Cambia el puerto RTSP y el método de transporte en la **Network** setting. Para obtener detalles sobre la configuración del puerto, la transmisión de video y la configuración de cifrado, consulta el siguiente documento.

- Ajustes de puertos
- Ajustes de transmisión y cifrado de video

> **Información**
> Si cambiaste el puerto RTSP respecto al valor predeterminado (554), ingresa el número de puerto cambiado en la parte `{port}` de la **URL de conexión** a continuación.

URL de conexión RTSP

Para obtener video de la cámara mediante RTSP en un NVR/VMS de terceros, registra una URL de conexión que coincida con el canal y la resolución.

Canal	Transmisión	URL de conexión
Canal 1 - Fisheye (video fisheye)	Transmisión principal (alta resolución)	`rtsp://{id}:{passwd}@{IP_address}:{port}/fisheye_primary`
Canal 1 - Fisheye (video fisheye)	Transmisión secundaria (baja resolución)	`rtsp://{id}:{passwd}@{IP_address}:{port}/fisheye_secondary`
Canal 2 - Dewarp (video rectificado)	Transmisión principal (alta resolución)	`rtsp://{id}:{passwd}@{IP_address}:{port}/dewarp_primary`

- `{id}`, `{passwd}`: Ingresa el ID y la contraseña de la cuenta usada para acceder a la cámara.
- `{IP_address}`: Ingresa la dirección IP de la cámara.
- `{port}`: Ingresa el número de puerto RTSP. El valor predeterminado es 554.

Integración ONVIF

Especificaciones admitidas

La cámara admite ONVIF **Profile S** y **Profile T**.

Prepara una cuenta ONVIF dedicada

Según las especificaciones del estándar de seguridad, la cuenta de administrador predeterminada (admin) no admite conexiones ONVIF. Antes de integrar con ONVIF, agrega una cuenta de operador dedicada para ONVIF y usa la información de esa cuenta para acceder al NVR/VMS. Consulte Configurar Ajustes de Red para obtener instrucciones para agregar una cuenta de operador solo de ONVIF.

Notas de integración

- **Proteger la sincronización de la configuración**

  Para mantener la coherencia de datos con el motor de configuración web y evitar fallas, no se admiten las operaciones de escritura que cambian la configuración interna de la cámara, como la resolución, la tasa de bits y las propiedades del sensor de imagen, mediante ONVIF.

- **Desactiva la función de optimización automática de VMS**

  Algunos productos VMS incluyen una función que cambia automáticamente la configuración de la cámara al

conectarse, como Video Optimization y Auto Configuration. Si esta función está habilitada, pueden producirse errores de integración, así que desactiva en el VMS la opción de corrección/optimización automática para la configuración de la cámara.

Precaución

Si cambias el método de transporte RTSP, quizá debas volver a conectar la sesión RTSP existente. Configura el NVR/VMS para que sea compatible con el método de transporte seleccionado.

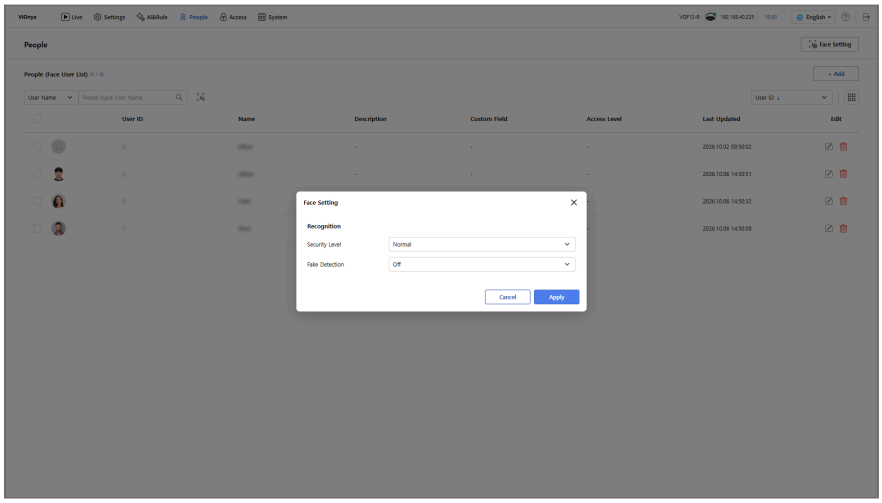
Administrar Usuarios

Enrolle usuarios para habilitar la feature de reconocimiento facial con IA. Administre de forma eficiente todo el ciclo de vida de los usuarios, desde el enroll de nuevos usuarios hasta la administración y visualización de la información de usuarios existentes.

Configurar Autenticación Facial

Use la configuración de Autenticación facial para administrar a la vez la eficiencia de la autenticación, el nivel de seguridad y la detección de suplantación. Ajuste los valores según la política de seguridad y el entorno operativo de su organización.

1. Haga clic en el menú **People** en la esquina superior izquierda de la pantalla.
2. Haga clic en **Face Setting** en la esquina superior derecha de la pantalla.
3. Cuando aparezca la ventana **Face Setting**, configure las opciones requeridas.



   - **Security Level**: Configure el nivel de seguridad. Cuanto mayor sea el nivel de seguridad, más estricta será la autenticación.
   - **Fake Detection**: Evite la autenticación de usuarios con rostros falsificados, como fotografías.
4. Cuando termine de configurar las opciones, haga clic en **Apply**.

> **Consejo**
> Para áreas que requieren alta seguridad, establezca la opción **Security Level** en **Most Secure**.

Agregar usuarios

Enrolla usuarios para Autenticación Facial con IA. Al agregar un usuario, ingresa la información básica y enrolla un rostro mediante uno de tres métodos.

Agrega usuarios en las siguientes situaciones.

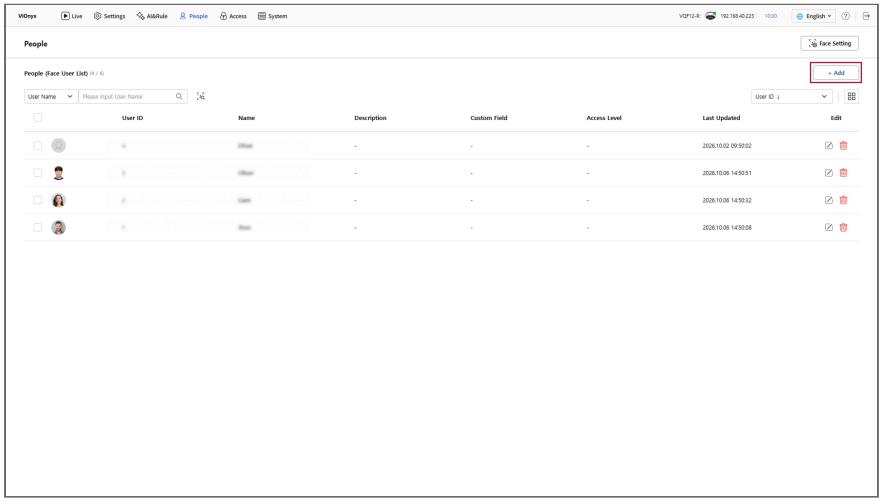
- Al enrollar a un nuevo empleado en la organización
- Al enrollar la foto del rostro de un usuario en la base de datos de Autenticación Facial
- Al agregar varios usuarios en lote
- Al enrollar usuarios para la integración con sistemas externos (ERP, sistema de gestión de RR. HH.)

> **Información**
>
> - Para usar la función de Facial Authentication, cumpla con las normas locales.
> - Al agregar el primer usuario, aparece una ventana emergente de consentimiento de Autenticación Facial. El registro del sistema almacena los consentimientos; la ventana emergente no vuelve a aparecer después del consentimiento.
> - Si el consentimiento se completó antes en la configuración de Eventos de IA, no aparece ninguna ventana emergente al agregar usuarios.

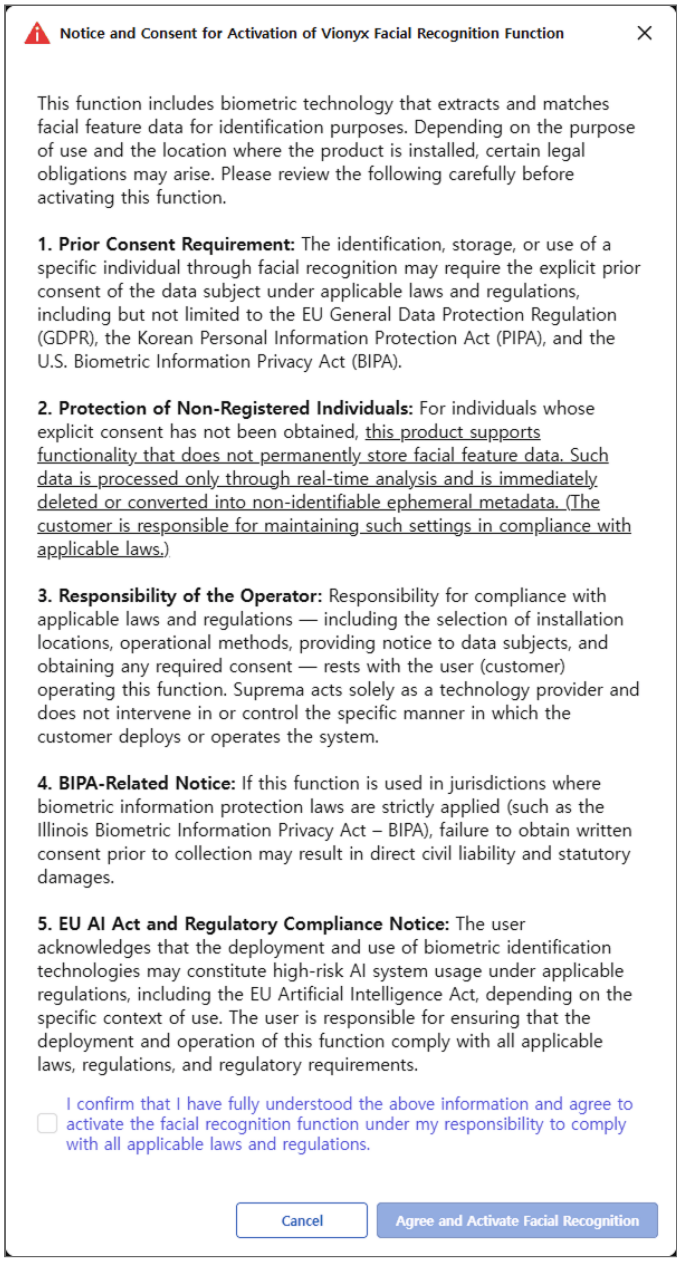
Ingresa la información básica del usuario

Si aparece la ventana emergente de consentimiento de Autenticación Facial al agregar al primer usuario, revisa el contenido y continúa. Después de dar el consentimiento, ingresa la información básica en el cuadro de diálogo Agregar usuario.

1. Haga clic en el menú **People** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Add** en la esquina superior derecha de la pantalla.

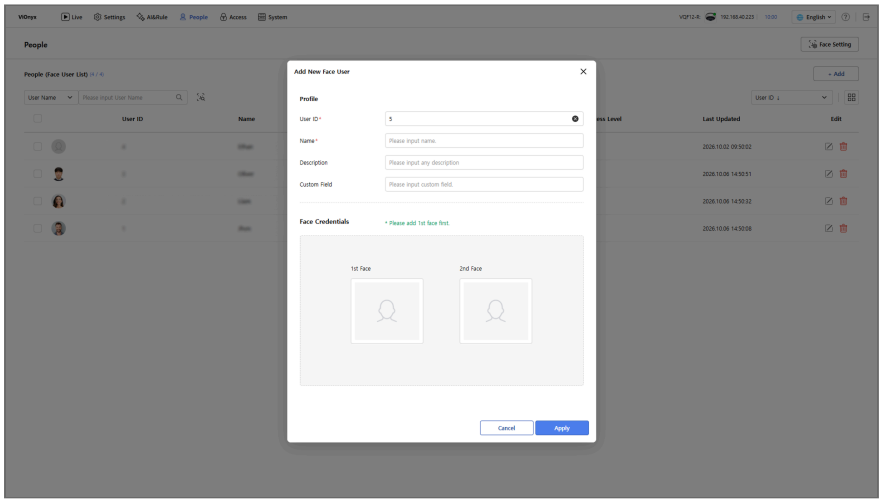


3. Al agregar al primer usuario, si aparece la ventana emergente **Notice and Consent for Activation of Vionyx Facial Recognition Function**, revisa el contenido, selecciona la casilla de consentimiento y haz clic en **Agree and Activate Facial Recognition**.



- Para usar la función de Facial Authentication, cumpla con las normas locales. No puede continuar sin consentimiento.
- La ventana emergente **Notice and Consent for Activation of Vionyx Facial Recognition Function** aparece solo una vez.

4. Cuando aparezca la ventana emergente **Add New Face User**, ingresa la información básica del usuario.



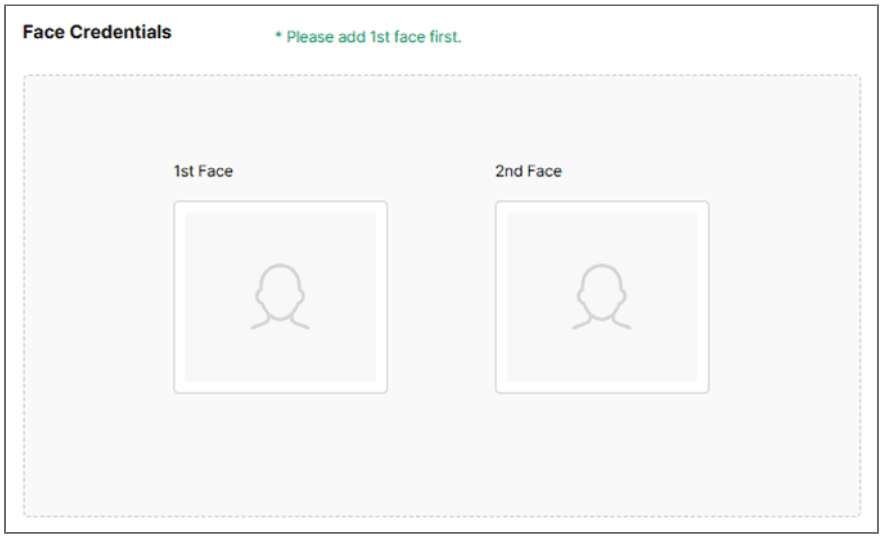
5. Ingresa el ID único del usuario en el campo **User ID**. El ID de usuario debe ser único.
6. Ingresa el nombre del usuario en el campo **Name**.
   - Hasta 64 caracteres.
   - Puede incluir letras coreanas, japonesas e inglesas en mayúsculas y minúsculas, números, caracteres especiales (`#`, `-`, `_`, `.`, `(`, `)`), y espacios dentro de una palabra.
7. Ingresa una descripción del usuario en el campo **Description**. Ingresa hasta 256 caracteres.
8. El campo **Custom Field** permite ingresar hasta 64 caracteres de información adicional específica del usuario. Por ejemplo, ingresa notas en inglés como departamento, cargo o grupo de usuarios.
9. Haz clic en **Apply** para guardar la información básica del usuario.

> **Información**
>
> Crea usuarios nuevos sin una foto de rostro. Agrega una foto de rostro más tarde desde la página de detalles del usuario.

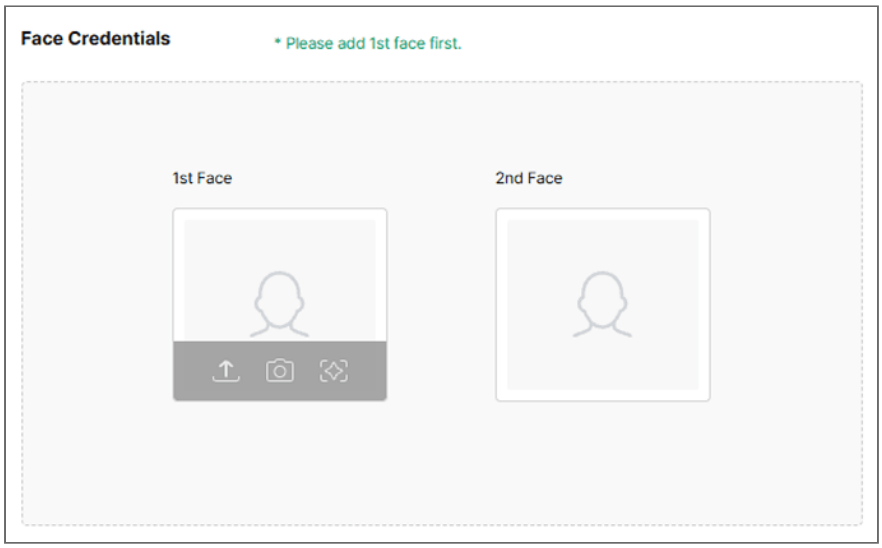
Enrolamiento facial

Enrolla un rostro al agregar un usuario nuevo o desde la página de detalles del usuario. Hay tres métodos disponibles.

1. Haga clic en el menú **People** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Add** en la esquina superior derecha de la pantalla o haz clic en un usuario existente de la lista de usuarios para abrir la página de detalles.
3. Enrolla un rostro en la sección **Face Credentials** del cuadro emergente Agregar usuario o Detalles del usuario.



4. Pasa el cursor sobre **1st Face** para mostrar las opciones de enrollamiento.

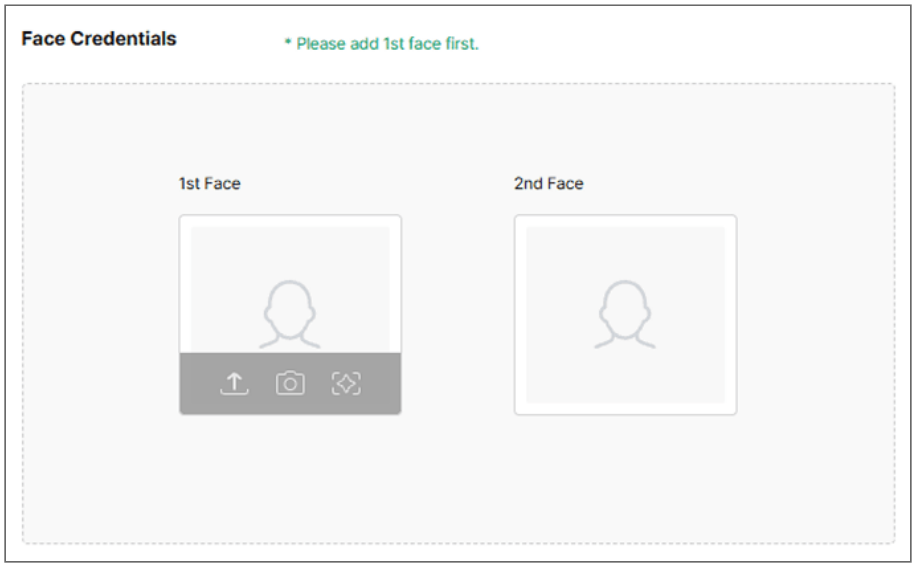


- : Sube un archivo de imagen guardado localmente para enrollar una foto de rostro.
- : Captura una foto de rostro con una cámara web para enrollarla.
- : Selecciona un rostro que coincida con el usuario de la lista de rostros no reconocidos detectados mediante eventos de IA y enrolla ese rostro.

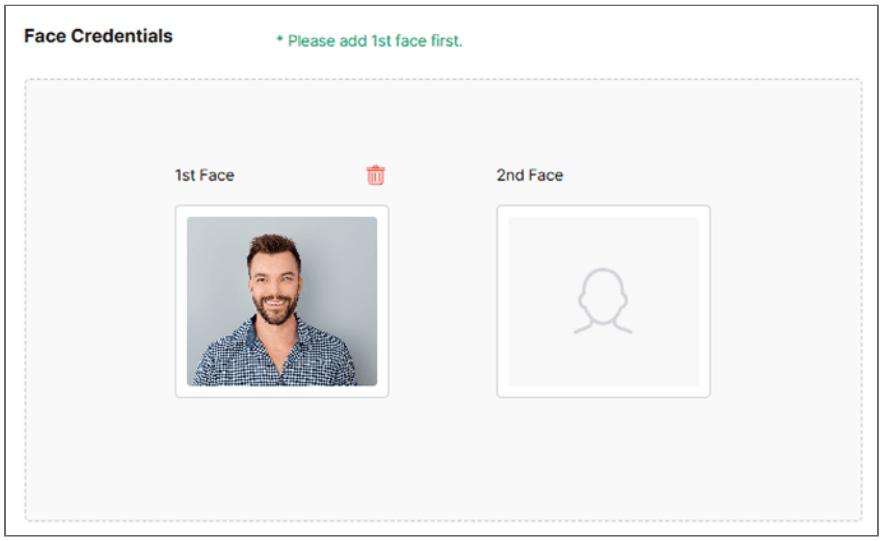
> **Información**
> Primero selecciona la ranura de rostro 1. La ranura de rostro 2 es opcional.

Subir foto de rostro

Sube un archivo de imagen guardado localmente para enrollar una foto de rostro.



1. Sube la foto de rostro mediante uno de los siguientes métodos.
   - Arrastra y suelta un archivo de imagen guardado localmente sobre el área del rostro.
   - Para seleccionar un archivo de imagen guardado localmente, haz clic en y elige el archivo de imagen que quieras.
2. Cuando se detecta el rostro, aparece la foto.



3. Para aplicar la foto subida al usuario, haz clic en **Apply** en la parte inferior.

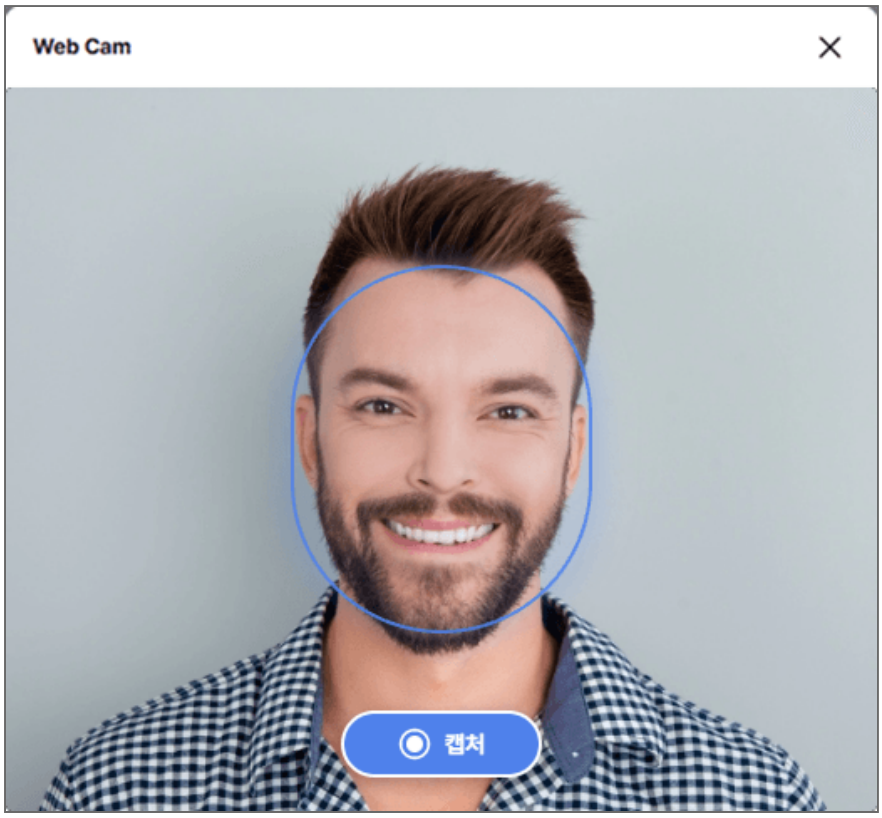
> **Información**
>
> - Los formatos de imagen admitidos son PNG, JPEG y JPG.
> - El tamaño máximo de los archivos de imagen admitidos es de 10 MB.

Enrollar rostro con cámara web

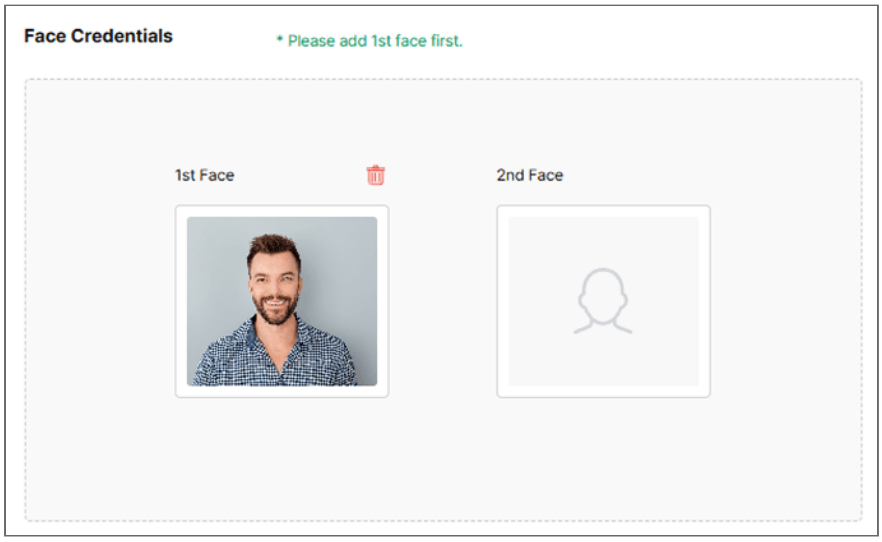
Usa una cámara web para capturar y enrollar una foto de rostro.

1. Haz clic en .

2. Cuando aparezca la pantalla de captura de la cámara web, coloca tu rostro dentro del círculo central.



3. Haz clic en **Capture**.



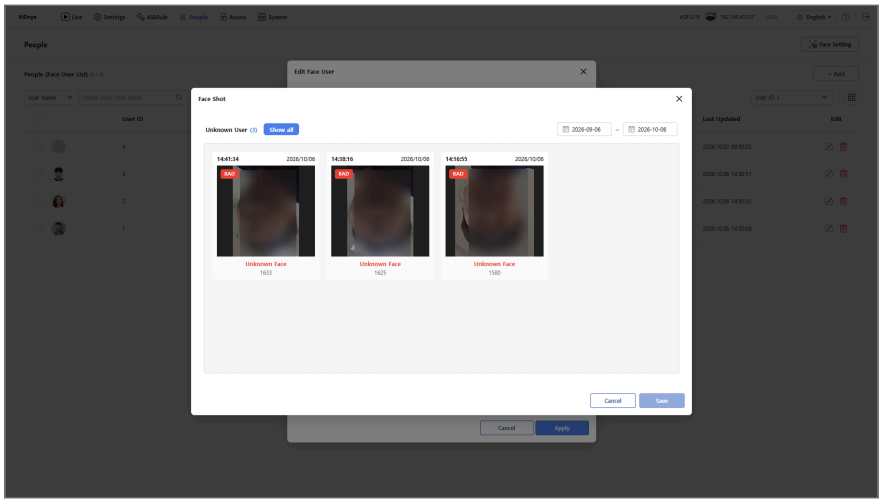
4. Para aplicar la foto capturada al usuario, haz clic en **Apply**.

> **Información**
> Para capturar de nuevo, haz clic en la foto de rostro y vuelve a capturarla.

Enrollar rostro recomendado por IA

Seleccione y enrolle un rostro que coincida con el usuario de la lista de rostros no enrollados detectados mediante análisis de IA.

1. Haz clic en .
2. La ventana emergente **Face Shot** muestra la lista de rostros no enrollados autenticados recientemente.



   Si no aparece la lista **Enrollable faces**, haga clic en **Show all**. Ver todos los rostros no enrollados.
3. Selecciona el rostro que coincide con el usuario. Solo se puede seleccionar un rostro a la vez.
4. Haz clic en **Save**.
5. Haz clic en **Apply** para aplicar al usuario el rostro seleccionado.

Editar y Eliminar Usuarios

Edita la información de un usuario registrado o agrega o cambia un rostro. Elimina a los usuarios que ya no se necesitan y revisa el historial de actividad de un usuario en el registro de eventos.

Modifica o elimina usuarios en las siguientes situaciones.

- Cuando necesitas cambiar el nombre, el departamento u otra información de un usuario
- Cuando necesitas actualizar la foto de rostro de un usuario o agregar un nuevo rostro
- Cuando un usuario deja la empresa o debe eliminarse del sistema
- Cuando necesitas revisar los registros de autenticación y el historial de cambios de un usuario
- Cuando ocurre una autenticación falsa para un usuario registrado

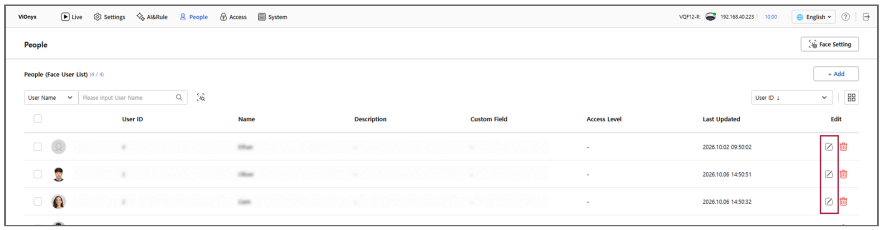
Información

- Aunque cargues una foto de alta calidad al editar la información del usuario, los datos de plantilla anteriores pueden permanecer. Elimina al usuario y regístralo de nuevo.
- La eliminación no se puede deshacer. Haz una copia de seguridad de los datos necesarios y verifica cuidadosamente antes de eliminar a un usuario.

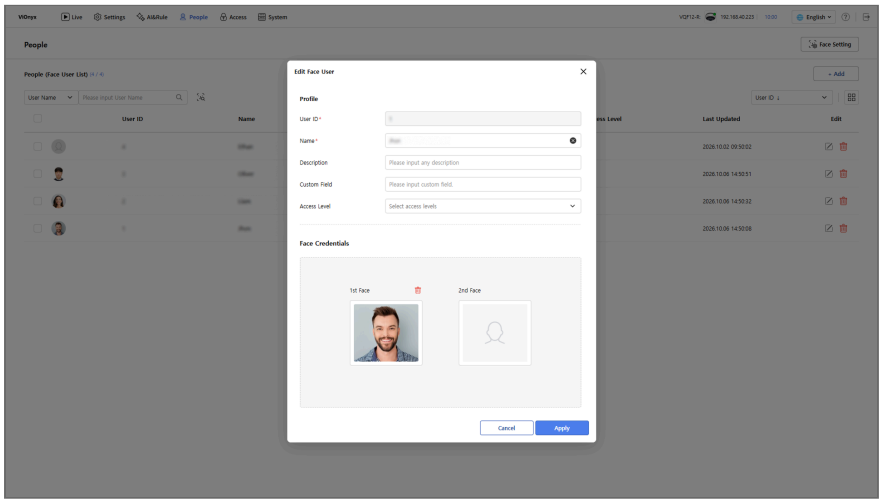
Editar información del usuario

Edita la información de un usuario registrado o agrega o cambia un rostro.

1. Haga clic en el menú **People** en la esquina superior izquierda de la pantalla.
2. En la lista de usuarios, haz clic en el botón de la columna **Edit** del usuario que deseas editar.



3. Cuando aparezca la ventana **Edit Face User**, edita la información requerida.



4. Después de editar la información del usuario, haz clic en **Apply**.

Después de guardar los cambios, aparece un mensaje de éxito en la parte superior derecha y la vista vuelve a la lista de usuarios.

> **Información**
>
> - Para obtener más información sobre los datos del usuario, consulta Agregar usuarios.
> - El **User ID** no se puede cambiar.
> - Las fotos de rostro se pueden eliminar individualmente. Haz clic en en la esquina superior derecha de esa foto de rostro.

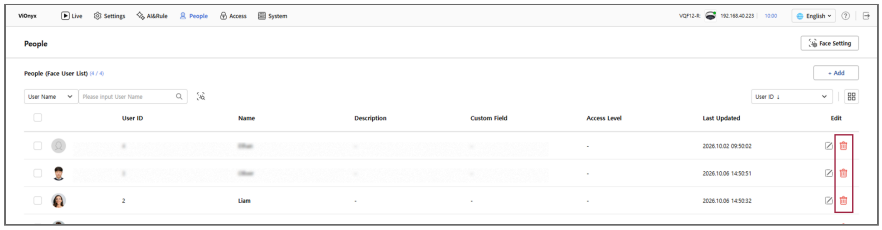
Eliminar usuarios

Elimina a los usuarios que ya no se necesitan.

Eliminar un usuario individual

1. Haga clic en el menú **People** en la esquina superior izquierda de la pantalla.

2. En la lista de usuarios, haz clic en al extremo derecho del usuario que deseas eliminar.

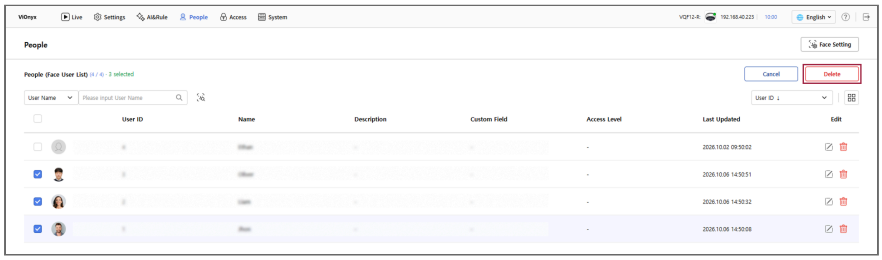


3. Cuando aparezca el mensaje de confirmación de eliminación, haz clic en **OK**.

Aparece un mensaje de confirmación de eliminación en la parte superior derecha y el usuario se quita de la lista de usuarios.

Eliminar varios usuarios

1. Haga clic en el menú **People** en la esquina superior izquierda de la pantalla.
2. En la lista de usuarios, haz clic en la casilla de verificación al extremo izquierdo del usuario que deseas eliminar. Selecciona varios usuarios.



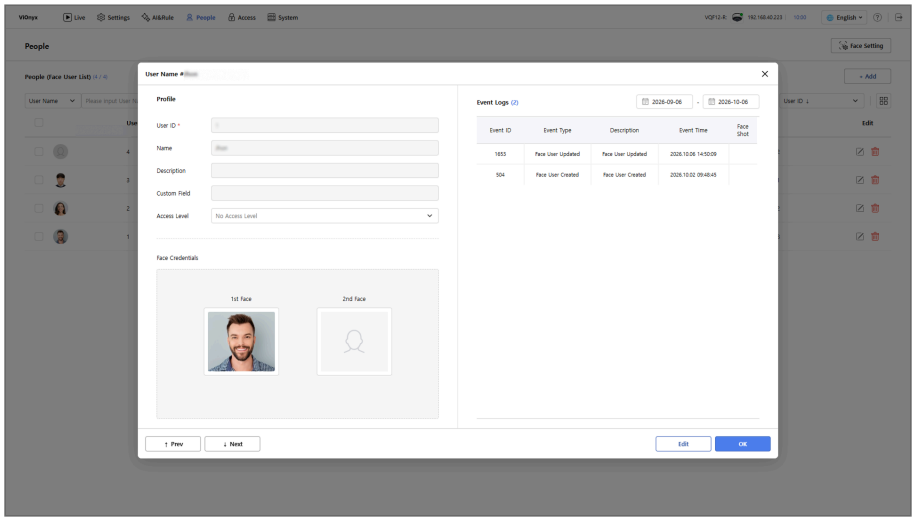
3. Cuando aparezca el botón de eliminar en la parte superior derecha de la pantalla, haz clic en **Delete**.
4. Cuando aparezca el mensaje de confirmación de eliminación, haz clic en **OK**.

Aparece un mensaje de confirmación de eliminación en la parte superior derecha y el usuario se quita de la lista de usuarios.

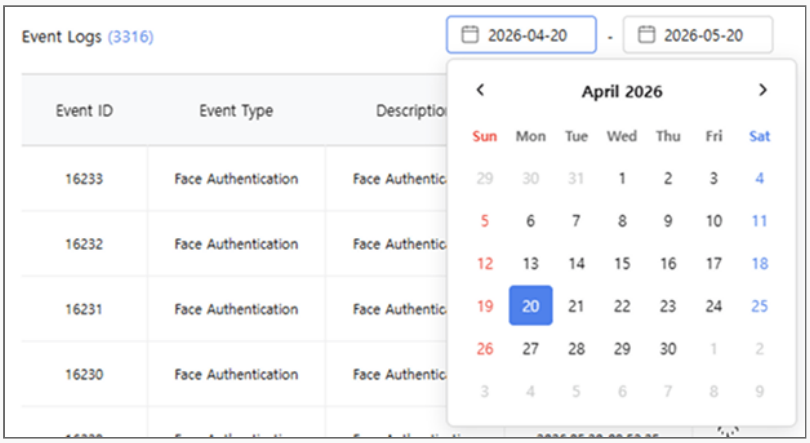
Ver registros de eventos de usuario

Ver el historial de actividad de los usuarios registrados en el registro de eventos.

1. Haga clic en el menú **People** en la esquina superior izquierda de la pantalla.
2. En la lista de usuarios, haz clic en el usuario para ver el registro de eventos.
3. Cuando aparezca la ventana emergente de detalles del usuario, revisa la lista de eventos a la derecha, en **Event Logs**.



- Usa el ícono de calendario en la parte superior derecha para ver eventos de una fecha específica.



- Los registros de eventos se guardan automáticamente y rastrean todas las actividades importantes del usuario.

Búsqueda y Vista de Usuarios

Ingrese un nombre o ID en la lista de usuarios para encontrar rápidamente a un usuario. Cambie entre las vistas de tabla y tarjeta para mostrar la información del usuario según sea necesario.

Use la función de búsqueda y vista de usuarios en las siguientes situaciones.

- Cuando necesita encontrar rápidamente a un usuario específico entre muchos usuarios
- Cuando necesita ver los perfiles de usuario de un vistazo en la vista de tarjeta
- Cuando quiere ordenar la lista de usuarios por nombre, ID y hora de la última actualización

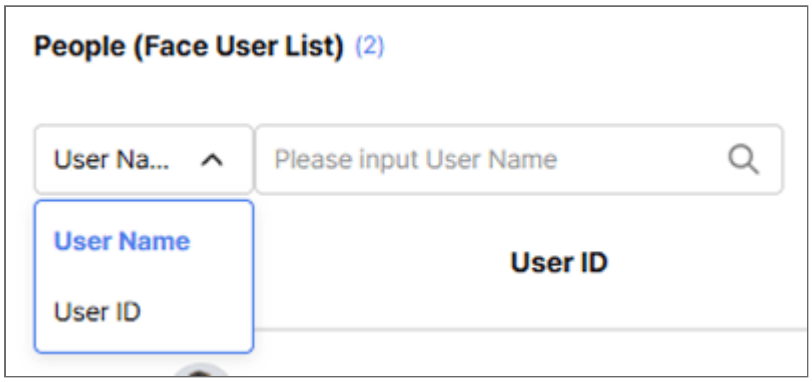
Búsqueda de usuarios

Ofrece una función de búsqueda para encontrar al usuario que necesita. Busque por nombre o ID de usuario, o encuentre usuarios similares por imagen facial.

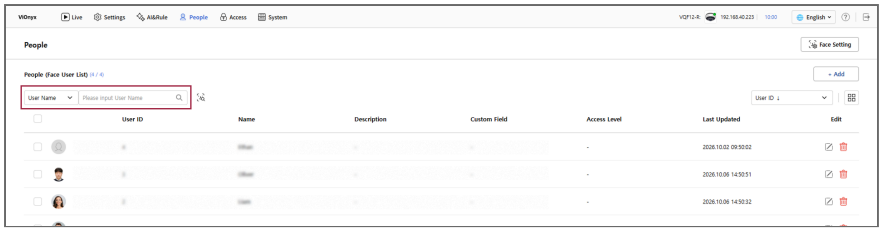
Búsqueda por palabra clave

Ingrese un nombre o ID en la lista de usuarios para buscar al usuario que necesita.

1. Haga clic en el menú **People** en la esquina superior izquierda de la pantalla.
2. Seleccione los criterios de búsqueda en el campo de búsqueda en la parte superior izquierda de la lista de usuarios. Seleccione **User Name** o **User ID**.



3. Ingrese un término de búsqueda en el campo de búsqueda.



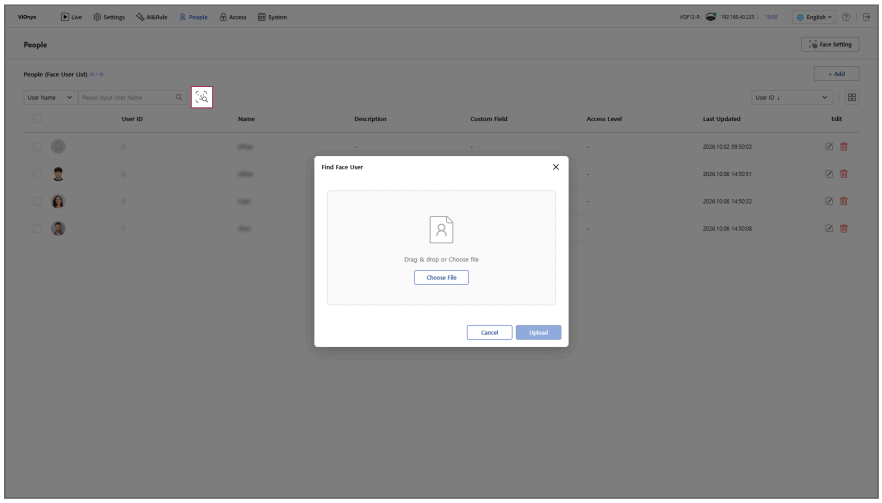
4. Los usuarios que coincidan con el término de búsqueda ingresado aparecen en la lista.

> **Información**
>
> - Admite búsqueda parcial. Por ejemplo, al ingresar 'Kim' se muestran todos los usuarios cuyos nombres incluyen 'Kim'.
> - Los filtros seleccionados actualmente determinan los resultados de búsqueda. Cambie los filtros para actualizar los resultados de búsqueda en consecuencia.

Buscar por imagen facial

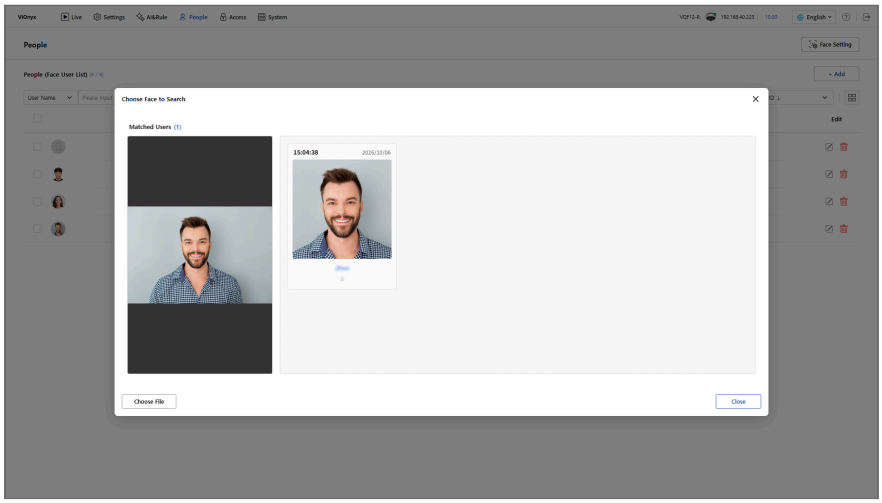
Cargue una imagen facial para buscar usuarios con un rostro similar.

1. Haga clic en el menú **People** en la esquina superior izquierda de la pantalla.
2. Haga clic en a la derecha del campo de búsqueda.
3. Cuando aparece la ventana **Find Face User**, arrastre y suelte una imagen facial o cárguela mediante **Choose File**.



4. Después de completar la carga de la imagen facial, haga clic en **Upload**.

5. Cuando aparece la ventana **Choose Face to Search**, aparece una lista de usuarios que coinciden con la imagen facial cargada.



- Seleccione el usuario deseado de los usuarios coincidentes para ir a la página de detalles de ese usuario.
- Para buscar otra vez con una imagen facial diferente, haga clic en **Choose File** en la parte inferior izquierda y cargue una nueva imagen facial.

> **Información**
>
> Si carga una imagen que no es facial, aparece un mensaje que indica que no es una imagen facial válida. Intente de nuevo con una imagen facial.

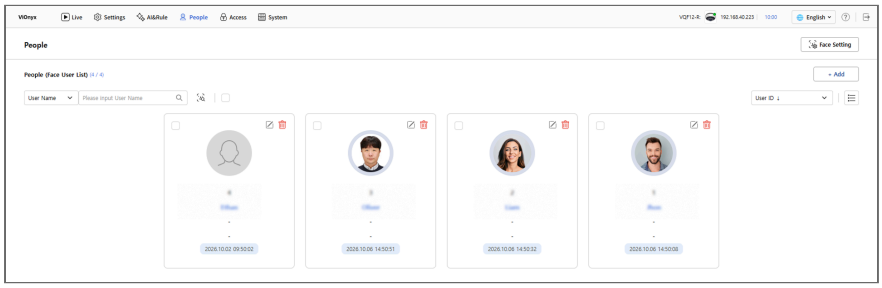
Cambiar modo de vista

Muestre la lista de usuarios en vista de tabla o de tarjeta. Haga clic en o en la parte superior derecha de la lista de usuarios para seleccionar el modo de vista que desea.

- **Switch to List View**



- **Switch to Grid View**

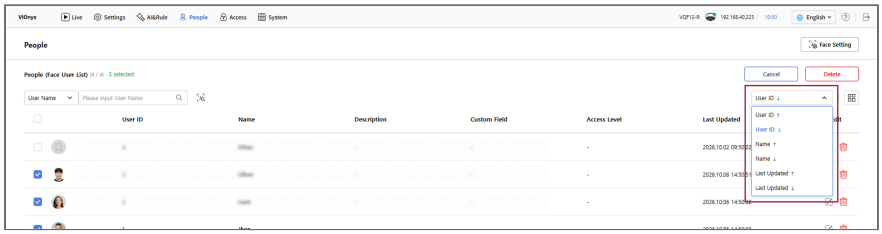


> **Información**
>
> **Switch to List View**, y **Switch to Grid View** ofrecen la misma función. Solo cambia la visualización; los resultados de búsqueda, filtrado y ordenación son idénticos.

Ordenamiento de la lista de usuarios

Ordene la lista de usuarios en orden ascendente o descendente por nombre de usuario, ID de usuario y hora de la última actualización.

1. Haga clic en la opción desplegable de ordenamiento en la parte superior derecha de la lista de usuarios.



2. Seleccione los criterios de ordenamiento deseados.

Administrar Control De Acceso

En el menú **Access**, agrega las puertas conectadas a la cámara. Define niveles de acceso para indicar quién accede a cada puerta y cuándo. Cuando un evento de control de acceso determina el permiso mediante la autenticación facial, la cámara abre el relé conectado a la puerta para otorgar acceso. Verifica el estado de la puerta en tiempo real y ábrela o bloquéala de forma remota. Configura mensajes de voz o notificaciones de webhook según la decisión de acceso. En la primera configuración, crea un evento y luego configura puertas, niveles y reglas, en ese orden.

Información

- La versión de firmware 1.1.0 o posterior incluye soporte para el menú **Access**.
- El menú **Access** está en versión beta. El diseño y el comportamiento de la pantalla pueden cambiar en futuras actualizaciones de firmware.

Administrar Puertas

Agregue puertas que la cámara desbloquea y bloquea. Al agregar una puerta, configure el evento de control de acceso, la salida del relé y el tiempo de apertura de la puerta. Agregue una puerta antes de seleccionarla en niveles de acceso y reglas de puertas.

Agregue la puerta en los siguientes casos.

- Abrir automáticamente la puerta para usuarios autenticados con autenticación facial
- Permitir que los usuarios abran la puerta desde el interior al presionar el botón de salida
- Verificar si la puerta está abierta o cerrada mediante un sensor
- Controlar la puerta por período, por ejemplo, desbloqueada durante el horario laboral y bloqueada por la noche

Antes de comenzar

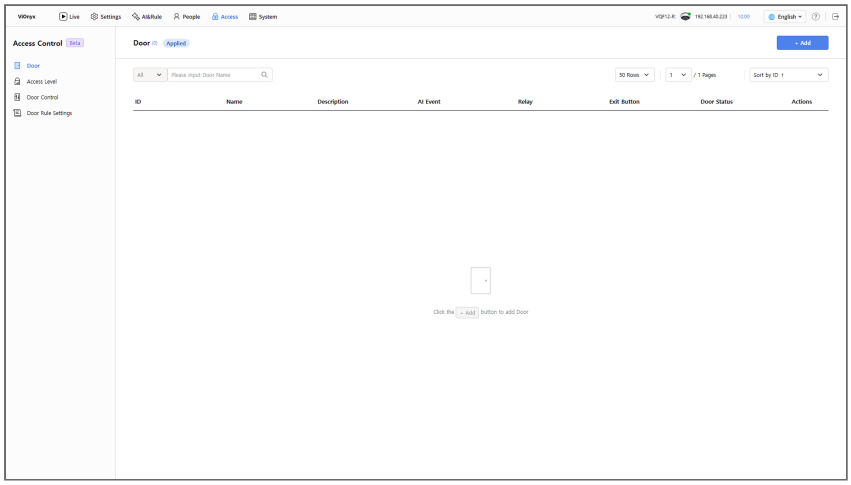
Revise lo siguiente antes de agregar una puerta.

- Cada cámara permite registrar hasta 10 puertas. Verifique cuántas puertas controlará la cámara antes de la configuración.
- Cree primero el evento de control de acceso para decidir el acceso. Para obtener más información, consulte Configurar Eventos De Control De Acceso.
- Asegúrese de que la cerradura de la puerta se conecte a un puerto de relé en la cámara o en el dispositivo de E/S secundario. Para usar un dispositivo de E/S secundario, agréguelo primero vía RS-485. Para obtener más información, consulte Configurar RS-485.
- Para usar un botón de salida o un sensor de estado de la puerta, asegúrese de que el dispositivo se conecte a un puerto de entrada.
- Cree horarios con anticipación para usar horarios de desbloqueo y bloqueo. Para obtener más información, consulte Administrar horarios.

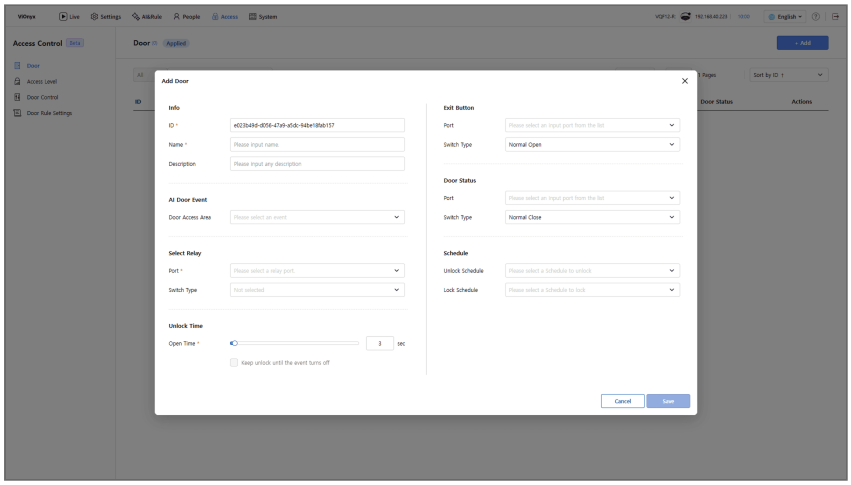
Agregar puertas

1 Comience a agregar puertas

1. Haz clic en el menú **Access** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Door** en la barra lateral izquierda.



3. Haga clic en **+ Add** en la esquina superior derecha de la pantalla.
4. Cuando aparezca la ventana emergente **Add Door**, ingrese la información de la puerta. Complete todos los campos obligatorios para habilitar el botón **Save**.



2 Ingrese información básica

En la sección **Info**, ingrese información para identificar la puerta.

- **ID**: Identificador único de la puerta. El sistema lo ingresa automáticamente. Cámbialo si es necesario. No use un ID que ya esté asignado a otra puerta. Ingresa hasta 64 caracteres. Usa letras, números, guiones (`-`) y guiones bajos (`_`).
- **Name**: Ingrese el nombre de la puerta. Obligatorio. No use el mismo nombre que otra puerta. Asigne un nombre según la ubicación, como **Entrada principal** o **Oficina del 2º piso**, para distinguir las puertas en niveles de acceso y reglas.

- **Description**: Ingrese una descripción para la puerta.

> **Información**
>
> - El ID y el nombre de la puerta deben ser únicos en el sistema. No use valores ya en uso.
> - Después de guardar, el ID de la puerta queda fijo.

3 Vincular eventos de control de acceso

En la sección **AI Door Event**, seleccione un área de control de acceso en la lista **Door Access Area** para usarla en la decisión de acceso de esta puerta. La lista muestra las áreas de control de acceso definidas al crear eventos de control de acceso.

> **Información**
>
> - Vincule cada área de control de acceso solo a una puerta. No seleccione un área ya vinculada a otra puerta.
> - La página Eventos de IA impide eliminar o cambiar el área de control de acceso vinculada a una puerta. Para cambiar el área, desvincúlela de la puerta primero.
> - Consulte Configurar Eventos De Control De Acceso para obtener más información sobre la creación de eventos de control de acceso.

4 Configurar relés

En la sección **Select Relay**, seleccione el relé que controla la cerradura de la puerta.

- **Port**: Seleccione el puerto del relé conectado a la cerradura de la puerta. Obligatorio. Seleccione un puerto de relé en la cámara o en un dispositivo de E/S aguas abajo. No seleccione puertos usados por otra puerta o regla de IA.
- **Switch Type**: Seleccione el tipo de contacto de la cerradura.
  - **Normal Open**: Normalmente abierto y se cierra cuando se activa el relé.
  - **Normal Close**: Normalmente cerrado y se abre cuando se activa el relé.

> **Precaución**
>
> - **Switch Type** se aplica al puerto del relé, no a la puerta. Al guardar una puerta, el sistema aplica el ajuste a todas las puertas y reglas que usan el puerto.
> - Verifique las especificaciones de la cerradura y seleccione el **Switch Type** correcto. Una selección incorrecta puede mantener la puerta desbloqueada durante el funcionamiento normal.

5 Ajuste del tiempo de desbloqueo

En la sección **Unlock Time**, defina cuánto tiempo mantener la puerta desbloqueada después de conceder el acceso.

- **Unlock Time**: Arrastre el control deslizante o ingrese un valor en el campo de entrada. Establezca de 1 a 120 segundos. Predeterminado: 3 segundos.
- **Keep unlock until the event turns off**: Seleccione esta opción para mantener la puerta desbloqueada hasta que finalice el evento de control de acceso, sin importar el tiempo de desbloqueo. Esta opción está disponible solo cuando selecciona un área de control de acceso.

> **Información**
>
> El ajuste **Condition** del evento de control de acceso determina cuándo finaliza el evento. Por ejemplo, para bloquear la puerta de inmediato cuando alguien entra detrás de otra persona sin autorización, seleccione **Keep until the area is clear or a tailgating violation occurs** en el evento de control de acceso. Para obtener detalles, consulte Configurar Eventos De Control De Acceso.

6 Ajustes del botón de salida (opcional)

Si el botón de salida está instalado en el interior de la puerta, defina el puerto de entrada conectado al botón en la sección **Exit Button**. El botón de salida abre la puerta sin autenticación facial.

- **Port**: Seleccione el puerto de entrada al que está conectado el botón de salida.
- **Switch Type**: Seleccione el tipo de contacto del botón de salida. El valor predeterminado es **Normal Open**.
  - **Normal Open**: Normalmente abierto y se cierra cuando se activa el relé.
  - **Normal Close**: Normalmente cerrado y se abre cuando se activa el relé.

7 Ajustes del estado de la puerta (opcional)

Si el sensor de posición de la puerta está instalado, defina el puerto de entrada conectado al sensor en la sección **Door Status**. Después de la configuración, la pantalla **Door Control** muestra si la puerta está abierta o cerrada.

- **Port**: Seleccione el puerto de entrada al que está conectado el sensor de posición de la puerta.
- **Switch Type**: Seleccione el tipo de contacto del sensor. El valor predeterminado es **Normal Close**.
  - **Normal Open**: Normalmente abierto y se cierra cuando se activa el relé.
  - **Normal Close**: Normalmente cerrado y se abre cuando se activa el relé.

> **Información**
>
> - Conecte el botón de salida y el sensor de estado de la puerta a puertos de entrada diferentes.
> - No seleccione un puerto de entrada que utilice otra puerta.

8 Ajustes de horario (opcional)

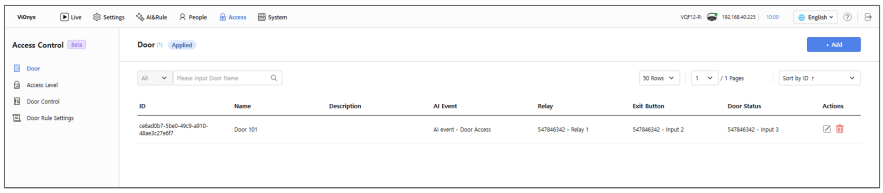
En la sección **Schedule**, configure la puerta para que quede desbloqueada o bloqueada por período de tiempo.

- **Unlock Schedule**: Mantenga la puerta desbloqueada durante el horario seleccionado. Úselo para mantener la puerta del vestíbulo desbloqueada durante las horas de mayor actividad.
- **Lock Schedule**: Mantenga la puerta bloqueada durante el horario seleccionado. Durante este intervalo, los usuarios inscritos no pueden acceder a la puerta. Sin embargo, las personas en el interior pueden salir al presionar el botón Salir.

> **Información**
>
> Use horarios distintos para abrir y bloquear. El sistema no puede guardarlos si las zonas horarias se superponen.

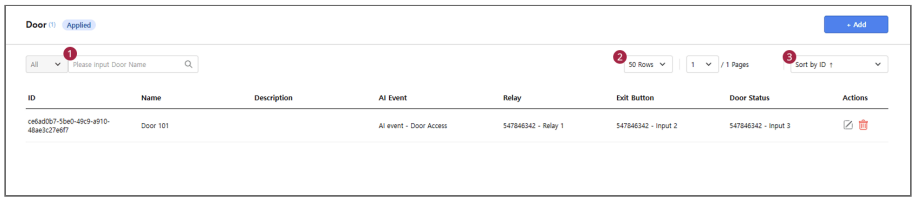
9 Guardar puerta

Después de completar todos los ajustes, haga clic en **Save**. El sistema agrega las puertas guardadas a la lista y las habilita en niveles de acceso y reglas de puertas.



Revisar lista de puertas

En la lista de puertas, revise las puertas guardadas y los eventos y puertos vinculados a cada puerta.



- Para encontrar una puerta específica, ingresa el nombre de la puerta en el campo de búsqueda (1).
- Selecciona un valor en la lista Filas por página (2) en la esquina superior derecha. Esto cambia el número de puertas por página.
- Para cambiar el criterio de ordenamiento, selecciona uno en **Sort by ID**(3).

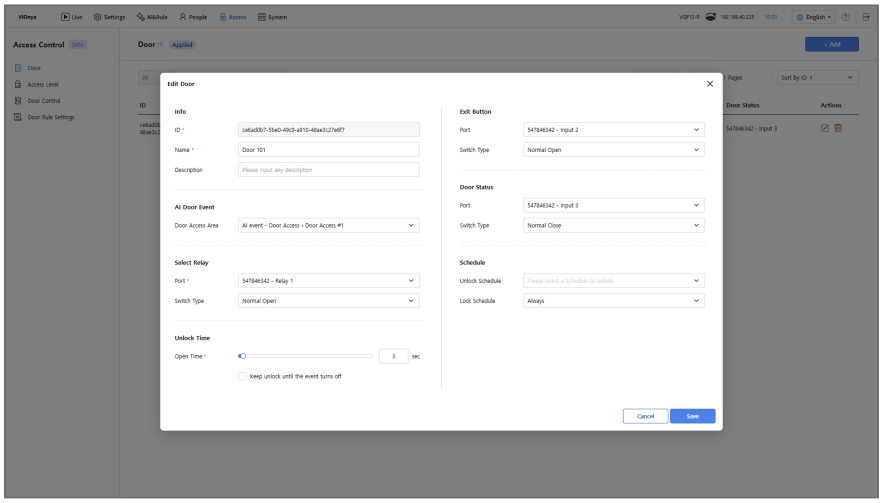
Los siguientes campos aparecen en la lista de puertas.

Ítem	Descripción
ID	El identificador único de la puerta.

Ítem	Descripción
Name	El nombre de la puerta.
Description	La descripción ingresada al agregar o editar la puerta.
AI Event	El área de control de acceso vinculada a la puerta.
Relay	Puerto de relé que controla la cerradura de la puerta.
Exit Button	Puerto de entrada conectado al botón de salida.
Door Status	Puerto de entrada conectado al sensor de apertura/cierre de la puerta.
Actions	Edite ( ) o elimine ( ) la puerta.

Editar puertas

1. En la lista de puertas, haga clic en el botón en el extremo derecho de la puerta para editarla.
2. Cuando aparezca la ventana emergente **Edit Door**, edite los campos.



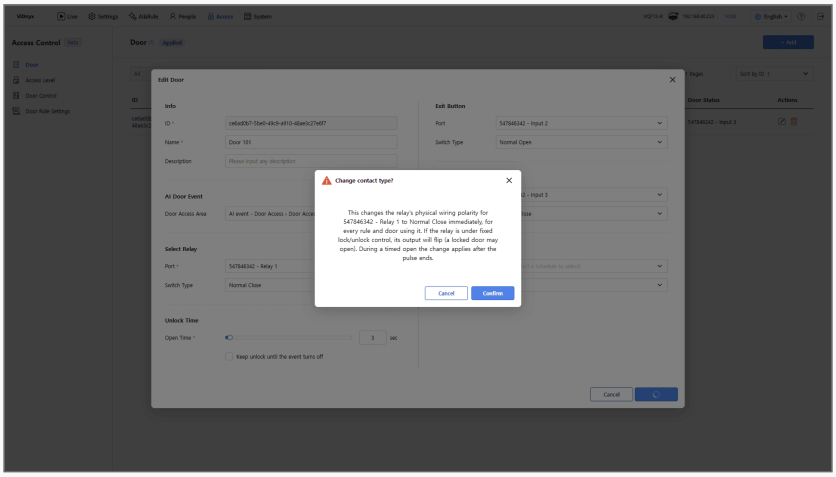
3. Haga clic en **Save** para guardar los cambios.

El sistema aplica los cambios de inmediato a los niveles de acceso y las reglas de puerta que usan la puerta.

> **Precaución**
>
> Si la puerta se bloquea o desbloquea manualmente, cambiar el **Switch Type** del relé podría invertir la salida y abrir una puerta bloqueada. Contrólela manualmente en el menú **Door Control** antes de cambiar el tipo de contacto.

Información

Cambie el **Switch Type** del relé y haga clic en el botón **Save**. Aparece un mensaje de confirmación.



- Haga clic en **OK** para cerrar el mensaje de confirmación y aplicar el nuevo tipo de contacto al puerto de relé de inmediato. También se aplica a todas las puertas y reglas que usan el puerto.
- Haz clic en **Cancel** para mantener el tipo de contacto y guardar solo los demás cambios.
- Si lo cambias mientras la puerta se mantiene abierta, se aplica cuando termina el tiempo de apertura.

Borrar puerta

1. En la lista de puertas, haz clic en al extremo derecho de la puerta para eliminarla.
2. Si aparece un mensaje de confirmación, revíselo y haga clic en **OK**.

Al borrar la puerta, el sistema la desvincula de los eventos de control de acceso conectados y de los niveles de acceso. La puerta borrada también desaparece de la lista **Door Control** y no se puede restaurar.

Información

- Al borrar una puerta que se usa en un nivel de acceso o una regla de puerta, el sistema también borra el nivel de acceso y la regla de puerta relacionados.
- Para agregar, editar o borrar puertas, necesitas el permiso **Read Write**. Si no tienes permiso, contacta a tu administrador. Para obtener más información sobre los roles de operador, consulta Administrar Operadores.

Siguiente paso

Después de agregar puertas, crea un nivel de acceso para definir cuándo ciertos usuarios pueden entrar.

Administrar Niveles de Acceso

Un nivel de acceso define **qué usuarios** pueden acceder a **qué puertas**, y **cuándo**. En los eventos de control de acceso, los

usuarios identificados mediante autenticación facial no pueden ingresar a menos que estén asignados al nivel de acceso de la puerta y dentro del horario de acceso.

Crea un nivel de acceso en las siguientes situaciones.

- Cuando solo ciertos departamentos o miembros del equipo deben tener acceso a una puerta
- Cuando debes establecer horarios de acceso diferentes para cada grupo de usuarios, como permitir el acceso solo en días hábiles y en horario laboral
- Cuando debes otorgar permisos separados a usuarios que acceden solo en ciertos periodos de tiempo, como los trabajadores del turno nocturno

Antes de comenzar

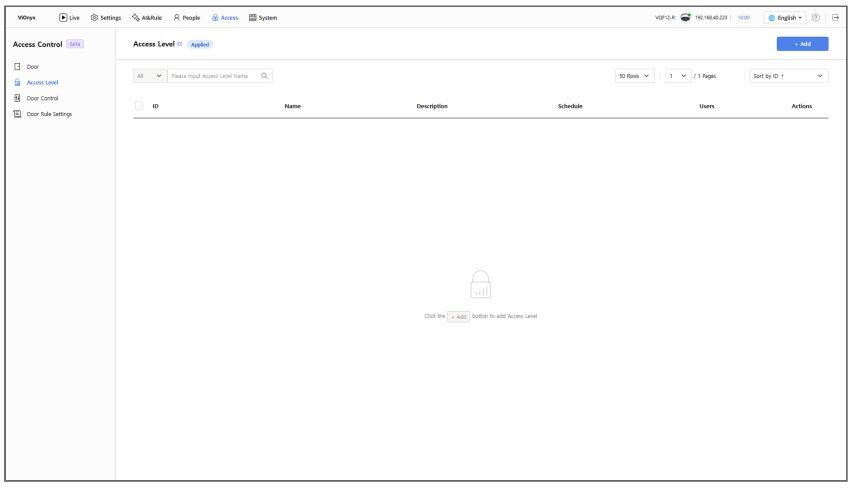
Antes de crear un nivel de acceso, revisa lo siguiente.

- Agrega puertas antes de asignarlas a un nivel de acceso. Para obtener más información, consulte Administrar Puertas.
- Inscribe a los usuarios con credenciales faciales antes de asignarlos al nivel de acceso. Para obtener más información, consulta Agregar usuarios.
- Crea horarios con anticipación para restringir el acceso por horario. Si no existe un horario, usa el horario predeterminado Siempre. Para obtener más información, consulte Administrar horarios.

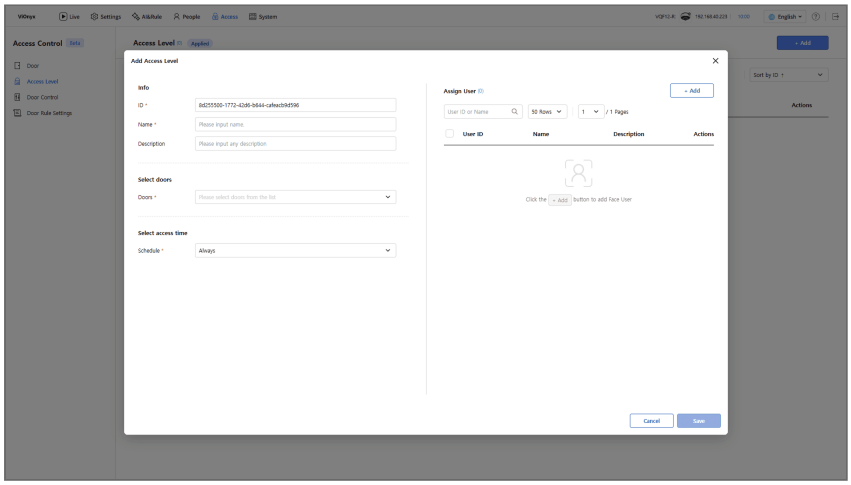
Agregar un nivel de acceso

1 Empieza a agregar un nivel de acceso

1. Haz clic en el menú **Access** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Access Level** en la barra lateral izquierda.



3. Haga clic en **+ Add** en la esquina superior derecha de la pantalla.
4. Cuando aparezca la ventana emergente **Add Access Level**, ingresa la información del nivel de acceso y luego asigna usuarios.



2 Ingrese información básica

En la sección **Info**, ingresa la información para identificar el nivel de acceso.

- **ID**: El ID único del nivel de acceso. El sistema lo ingresa automáticamente. Cámbialo si es necesario. No uses un ID que coincida con otro nivel de acceso. Ingresa hasta 64 caracteres. Usa letras, números, guiones (`-`) y guiones bajos (`_`).
- **Name**: Ingresa el nombre del nivel de acceso. Este campo es obligatorio. No use un nombre que coincida con otro nivel de acceso. Use un nombre que indique quién y cuándo, como **Equipo de desarrollo—acceso siempre** o **Trabajadores del turno nocturno**.
- **Description**: Ingrese una descripción para el nivel de acceso.

3 Seleccione puertas

En la sección **Select doors**, seleccione en la lista **Door** las puertas a las que permitirá el acceso. Obligatorio. Se pueden seleccionar varias puertas.

> **Información**
>
> Agregue al menos una puerta antes de seleccionar una puerta en la lista. Primero, agregue una puerta en **Access** → **Door**. Para obtener más información sobre el registro de puertas, consulte Administrar Puertas.

4 Seleccione horario de acceso

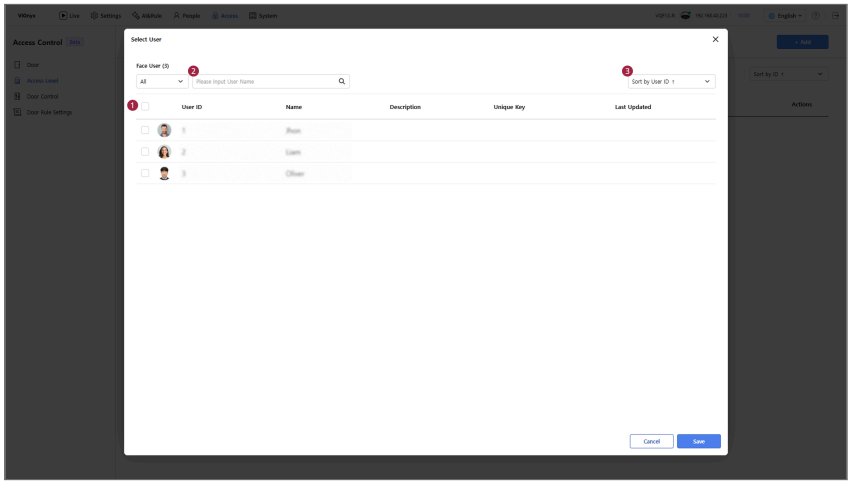
En la sección **Select access time**, seleccione un horario de la lista **Schedule** para permitir el acceso. Este campo es obligatorio. El valor predeterminado es **Siempre**. El sistema permite el acceso solo durante el horario seleccionado. El sistema niega el acceso en otros horarios, incluidos los usuarios inscritos.

> **Información**
>
> Para más información sobre la gestión de horarios, consulte Administrar horarios.

5 Asigne usuarios

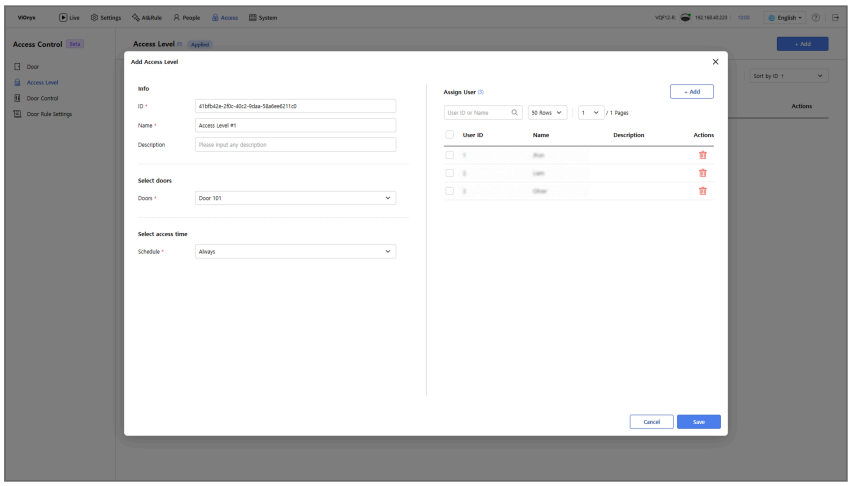
En la sección **Assign User**, agregue usuarios para aplicar el nivel de acceso.

1. Haga clic en **+ Add** en la esquina superior derecha de la sección **Assign User**.
2. Cuando aparezca la ventana emergente **Select User**, haga clic en la casilla de verificación de cada usuario que asignará.



- Seleccione la casilla de verificación (1) en el encabezado de la lista para seleccionar a todos los usuarios.
- Ingrese un nombre de usuario en el campo de búsqueda (2) para encontrar un usuario específico.
- Seleccione un criterio en la lista de ordenación (3) para cambiar el orden de clasificación.

3. Haz clic en **Save**. El sistema agrega los usuarios seleccionados a la lista **Assign User**.



Para quitar un usuario asignado del nivel de acceso, en la lista **Assign User**, haga clic en el botón de ese usuario.

> **Información**
>
> - La lista **Select User** muestra solo los usuarios inscritos con credenciales faciales.
> - Un usuario puede asignarse a varios niveles de acceso. Cada usuario puede asignarse a un número limitado de niveles de acceso.

6 Guardar nivel de acceso

Después de completar todos los ajustes, haga clic en **Save**. El sistema agrega el nivel de acceso guardado a la lista de niveles de acceso. Lo aplica de inmediato a los usuarios asignados.



Revisar la lista de niveles de acceso

La lista de niveles de acceso muestra niveles de acceso, horarios de acceso por nivel y usuarios asignados.



- Ingresa el nombre del nivel de acceso en el campo de búsqueda (1) para encontrar un nivel de acceso específico.
- Selecciona un valor en la lista Filas (2) en la parte superior derecha de la pantalla para cambiar la cantidad de niveles de acceso que aparecen por página.
- Para cambiar el criterio de ordenamiento, selecciona uno en **Sort by ID**(3).

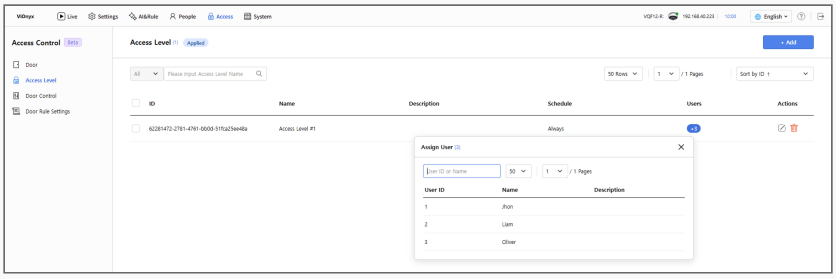
La siguiente información aparece en la lista de niveles de acceso.

Ítem	Descripción
ID	El identificador único del nivel de acceso.
Name	El nombre del nivel de acceso.
Description	La descripción ingresada al agregar o editar el nivel de acceso.
Schedule	El horario que permite el acceso.
User	La cantidad de usuarios asignados al nivel de acceso.

Ítem	Descripción
Actions	Edita ( ) o elimina ( ) niveles de acceso.

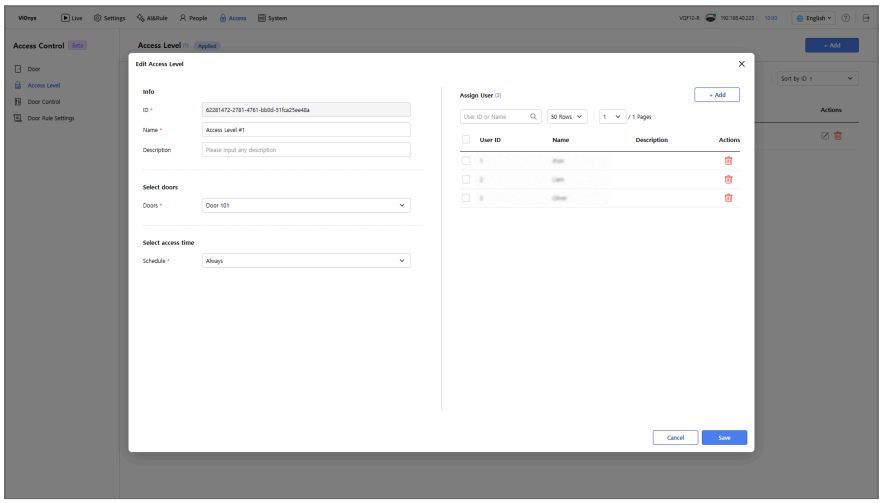
Información

Haz clic en el número en **User** para ver la lista de usuarios asignados.



Editar nivel de acceso

1. En la lista de niveles de acceso, haz clic en el botón a la derecha del nivel de acceso.
2. Cuando aparezca la ventana emergente **Edit Access Level**, edita las puertas, el horario de acceso y los usuarios asignados.



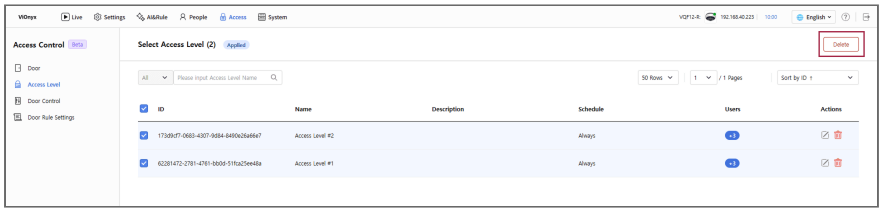
3. Haga clic en **Save** para guardar los cambios.

Al guardar los cambios, el sistema los aplica de inmediato a todos los usuarios asignados.

Borrar nivel de acceso

Elimina niveles de acceso de uno en uno o selecciona varios niveles de acceso para eliminarlos a la vez.

- **Eliminar uno**: En la lista de niveles de acceso, haz clic en al extremo derecho del nivel de acceso para eliminarlo.
- **Eliminar varios**: En la lista de niveles de acceso, selecciona las casillas de verificación de los niveles de acceso que vas a eliminar y haz clic en **Delete** en la parte superior derecha de la pantalla.



Si aparece un mensaje de confirmación, revíselo y haga clic en **OK**. Al eliminar un nivel de acceso, el sistema lo quita de todos los usuarios asignados. Las puertas y los usuarios no se eliminan. Los niveles de acceso eliminados no se pueden recuperar.

Precaución

Eliminar un nivel de acceso impide que los usuarios asignados solo a ese nivel accedan a las puertas. Revise los usuarios asignados antes de eliminar.

Siguiente paso

Defina reglas de puertas según decisiones de acceso: indicaciones de voz, notificaciones por webhook y luces de emergencia.

Controlar Puertas

En el menú **Door Control**, verifica en tiempo real el estado de bloqueo de las puertas registradas y abre o bloquea puertas de forma remota.

Controla la puerta directamente en las siguientes situaciones.

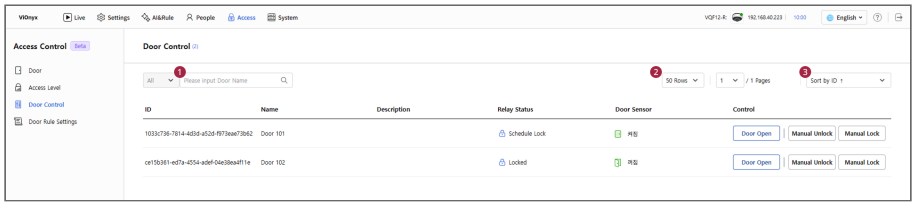
- Abre la puerta una vez para visitantes o repartidores sin credenciales faciales inscritas
- Mantén la puerta abierta para eventos o mudanzas
- Bloquea la puerta de inmediato en una emergencia, sin importar el horario

Información

- Se requiere una cuenta de operador para controlar las puertas. Sin permiso de operador, el sistema deshabilita la comprobación de estado y el control de puertas. Para obtener más información sobre los roles de operador, consulta Administrar Operadores.
- Para más información sobre cómo agregar y administrar puertas, consulta Administrar Puertas.

Verifica el estado de la puerta

1. Haz clic en el menú **Access** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Door Control** en la barra lateral izquierda.



La lista muestra las puertas registradas en el menú **Door**. La lista se actualiza de inmediato cuando agregas o eliminas una puerta.

- Para encontrar una puerta específica, ingresa el nombre de la puerta en el campo de búsqueda (1).
- Selecciona un valor en la lista Filas por página (2) en la esquina superior derecha. Esto cambia el número de puertas por página.
- Para cambiar el criterio de ordenamiento, selecciona uno en **Sort by ID**(3).

Los siguientes campos aparecen en la lista de puertas.

Ítem	Descripción
ID	El identificador único de la puerta.
Name	El nombre de la puerta.
Description	La descripción ingresada al agregar o editar la puerta.
Relay Status	El estado actual de la cerradura de la puerta.
Door Sensor	El estado actual del sensor de la puerta. Esta columna aparece solo cuando estableces el puerto de entrada **Door Status** de la puerta.
Control	Esta característica abre la puerta y la bloquea o desbloquea manualmente.

Estado del relé

La columna **Relay Status** muestra si la puerta de entrada está bloqueada y qué determina ese estado.

Estado	Descripción
Locked	La puerta de entrada permanece bloqueada de forma predeterminada.
Unlocked	La puerta de entrada permanece desbloqueada de forma predeterminada.
Schedule Lock	La puerta de entrada se bloquea según el horario de bloqueo.
Schedule Unlock	La puerta de entrada se desbloquea según el horario de desbloqueo.
Fixed Lock	Bloqueada con **Manual Lock**.

Estado	Descripción
Fixed Unlock	Desbloqueada con **Manual Unlock**.

Controlar puertas

Haz clic en el botón en la columna **Control** para controlar la puerta de entrada.

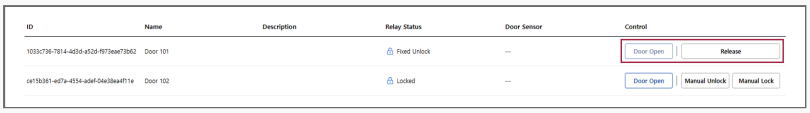
Botón	Activador y acción
Door Open	Abre la puerta de entrada una vez. La puerta de entrada vuelve a bloquearse cuando se agota el tiempo de apertura establecido.
Manual Unlock	Desbloquea la puerta de entrada y mantenla abierta hasta que ejecutes la característica **Release**.
Manual Lock	Bloquea la puerta de entrada y mantenla bloqueada hasta que ejecutes la característica **Release**. Durante este período, los usuarios inscritos no pueden ingresar y el botón Salir no abre la puerta.
Release	Finaliza **Manual Lock** o **Manual Unlock** y devuelve la puerta de entrada a su estado anterior.

Precaución

- En el estado **Manual Unlock**, cualquier persona puede acceder sin importar la autenticación facial. Después de completar las tareas requeridas, haga clic en el botón **Release**.
- En el modo **Manual Lock**, las personas que están dentro no pueden salir con el botón Salir. Antes de ejecutar **Manual Lock**, confirme que no quede nadie dentro.

Información

- El bloqueo manual o el desbloqueo manual deshabilitan el botón **Door Open** y muestran solo el botón **Release**.



- El control manual tiene prioridad sobre el horario de desbloqueo y el horario de bloqueo. Por ejemplo, al ejecutar **Manual Lock** durante un horario de desbloqueo, la puerta de entrada permanece bloqueada.
- Haz clic en **Release** para volver al horario vigente o al estado predeterminado.

Configurar Reglas de Puerta

Las reglas de puerta reproducen audio, envían webhooks o ejecutan acciones de relé según la decisión de acceso en la puerta. Cuando el sistema otorga acceso, la puerta se abre según los ajustes de la puerta. Defina acciones adicionales en reglas de puerta.

Configure reglas de puerta en las siguientes situaciones.

- Cuando suena un mensaje de bienvenida al otorgar acceso y un mensaje de instrucción al denegar acceso
- Cuando una persona no autorizada sigue a otra y debe activarse una luz de baliza o una alarma
- Cuando los registros de acceso deben enviarse a un sistema externo de control de acceso o a un servidor de monitoreo

Antes de comenzar

Antes de configurar reglas de puerta, revise lo siguiente.

- Agregue puertas antes de aplicar reglas. Para obtener más información, consulte Administrar Puertas.
- Cargue clips de audio antes de usar la reproducción de audio. Para obtener más información, consulte Subir Clips de Audio.
- Prepare la URL del receptor del webhook antes de usar webhooks.
- Conecte luces de baliza y alarmas al puerto de relé para usar relés. Para obtener más información sobre cómo conectar dispositivos externos, consulte la Guía de instalación de ViOnyx.

Resultados de decisiones de acceso

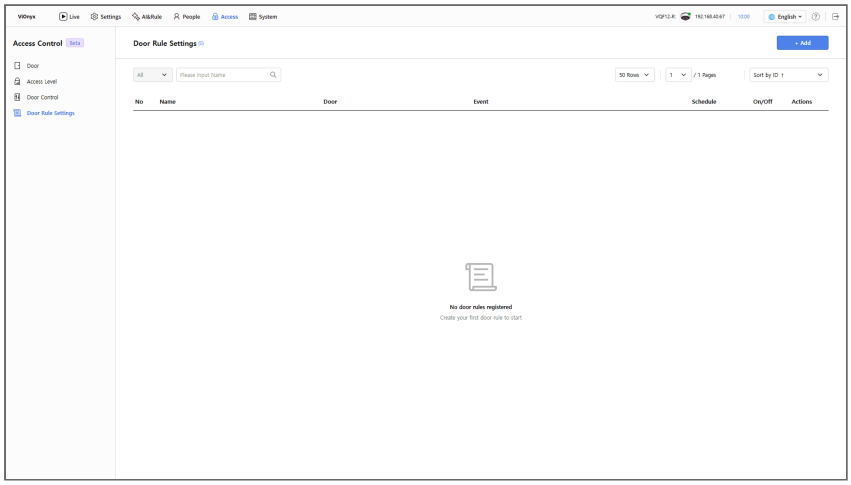
En las reglas de puerta, defina las acciones que el sistema ejecuta para cada resultado de decisión de acceso.

Resultados de decisiones de acceso	Condición de activación
Access Granted	El sistema identificó a un usuario con nivel de acceso durante el horario de acceso y otorgó acceso.
Access Denied by Unidentified	La autenticación facial no autenticó a la persona, o la persona no está inscrita.
Access Denied by Access Level	El sistema identificó a un usuario inscrito, pero el usuario no tiene el nivel de acceso de la puerta o está fuera del horario de acceso.
Access Denied by Door Mode (Manual/Schedule Lock)	El sistema denegó el acceso porque la puerta está bloqueada manualmente o por horario.
Access Denied by Anti-Tailgating	El sistema denegó el acceso porque la zona de verificación no cumplió la condición de tailgating o seguimiento.
Authenticated Passage (Door Line)	Un usuario al que se le otorgó acceso cruzó la línea de entrada del evento y entró.
Passage After Denial (Security Event)	Una persona con acceso denegado cruzó la línea de entrada del evento y entró. Este evento de seguridad indica un presunto ingreso forzado.

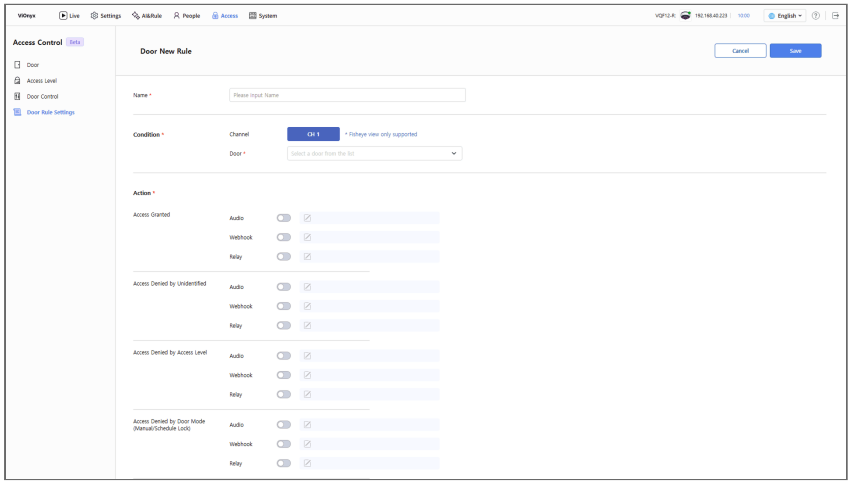
Añadir una regla de puerta

1 Iniciar la creación de una regla

1. Haz clic en el menú **Access** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Door Rule Settings** en la barra lateral izquierda.



3. Haga clic en **+ Add** en la esquina superior derecha de la pantalla.
4. Cuando aparezca la pantalla **Add Door Rule**, ingrese el nombre de la regla y configure las condiciones y acciones.



2 Ingresar nombre de la regla

Ingrese el nombre de la regla en el campo de entrada **Name**. Obligatorio.

3 Configurar condiciones

En la sección **Condition**, seleccione las puertas a las que se aplicará la regla.

- **Channel**: El canal está fijo en CH 1. Soporte solo para la vista ojo de pez.

- **Door**: Seleccione la puerta a la que se aplicará la regla. Obligatorio.

4 Configurar acciones

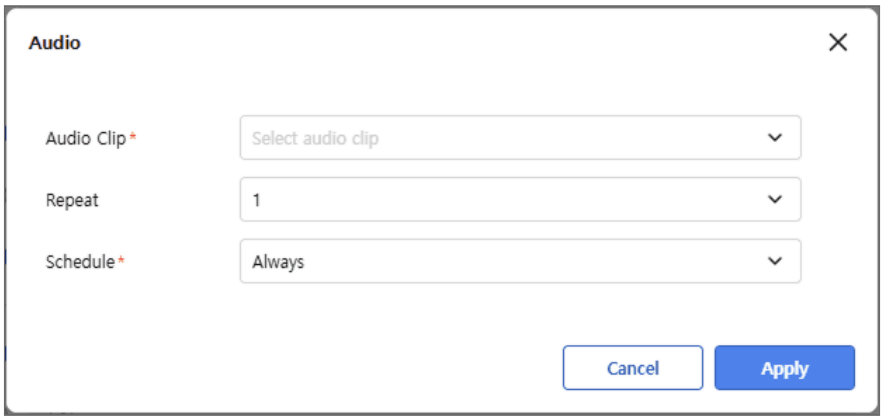
La sección **Action** muestra las acciones **Audio**, **Webhook** y **Relay** para cada resultado de decisión de acceso. Para el resultado de decisión de acceso que activa la acción, active el interruptor de la acción y haga clic en . Aparece la ventana emergente de ajustes de acción.

Active al menos 1 acción para guardar la regla. Consulte a continuación los ajustes específicos de cada acción.

> **Información**
> Fuera del horario de la acción, la acción no se ejecuta cuando ocurre un resultado de decisión de acceso. Administre los horarios en **AI&Rule** → **Schedule**. Para obtener más información, consulte Administrar horarios.

5 Ajustes de acción de audio

Cuando ocurre un resultado de decisión de acceso, la cámara reproduce un clip de audio.



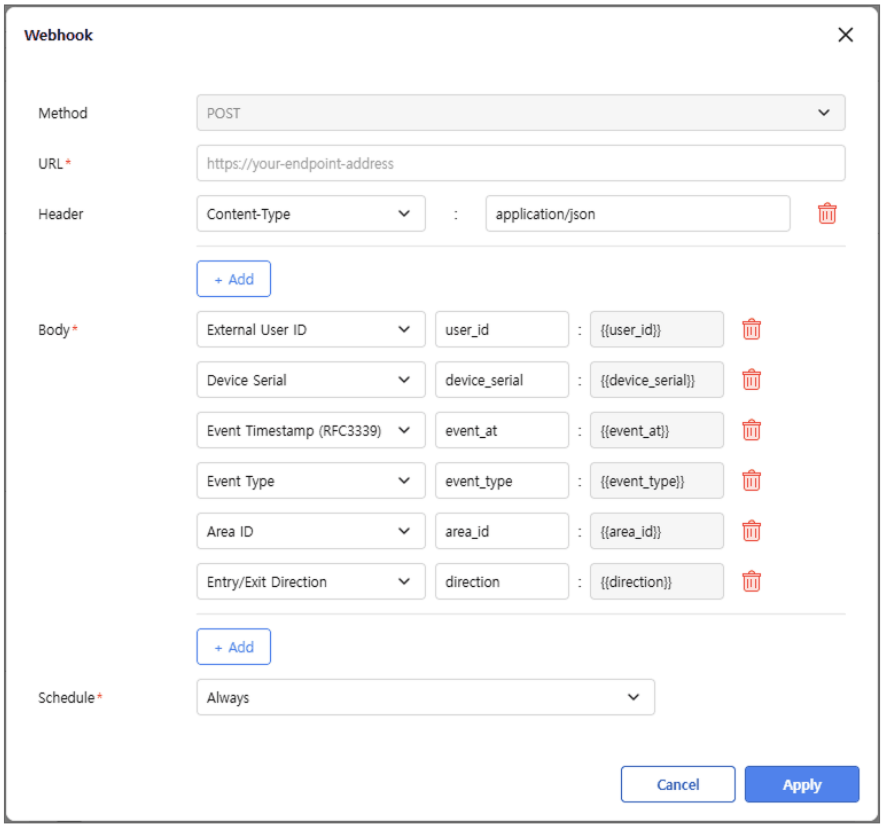
- **Audio Clip**: Seleccione el clip de audio que se reproducirá. Obligatorio.
- **Repeat**: Seleccione la cantidad de veces que se repetirá la reproducción de audio.
- **Schedule**: Seleccione el horario para la reproducción de audio. Obligatorio. El valor predeterminado es **Always**.

Haga clic en **Apply** para guardar los ajustes de la acción de audio.

> **Información**
> Prepare los clips de audio antes de configurar acciones de audio. Cargue clips de audio en **System** → **Audio**. Para obtener más información, consulte Subir Clips de Audio.

6 Ajustes de acción de webhook

Cuando ocurre un resultado de decisión de acceso, el sistema envía un webhook a un servidor externo.



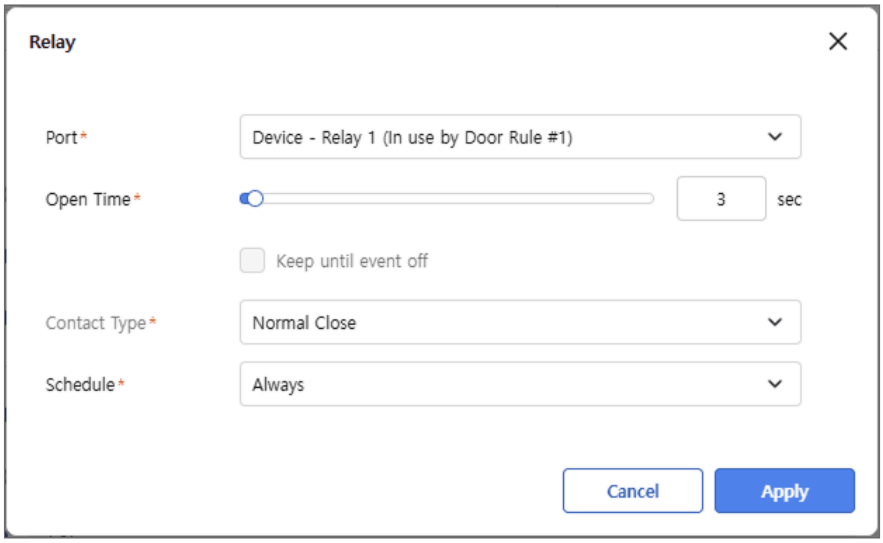
- **Method**: El método de transmisión del webhook. Solo se admite el método `POST`.
- **URL**: Ingrese la URL para recibir el webhook. Obligatorio.
- **Header**: Configure los encabezados HTTP que se incluirán en el webhook. El sistema agrega el encabezado `Content-Type: application/json` de forma predeterminada. Haga clic en **+ Add** para agregar encabezados. No use nombres de encabezados duplicados. No use nombres de encabezados reservados por el sistema.
- **Body**: Seleccione los campos que se incluirán en el cuerpo del webhook. Obligatorio. En cada fila, seleccione a la izquierda los datos para enviar e ingrese la clave JSON en el campo central. El campo derecho muestra variables que cambian a valores reales cuando ocurre un evento. Haga clic en **+ Add** para agregar un campo personalizado o haga clic en para eliminarlo. El tamaño máximo del cuerpo es 64KB.
- **Schedule**: Seleccione un horario para enviar webhooks. Obligatorio. El valor predeterminado es **Always**.

Para guardar la configuración, haga clic en **Apply**.

> **Información**
>
> - Por seguridad, los valores ingresados en el encabezado y el cuerpo no vuelven a aparecer después de guardar. Al editar una regla, los valores guardados se mantienen. Las nuevas entradas reemplazan los valores existentes.
> - Revise los resultados de entrega del webhook en el registro del sistema. Para obtener detalles, consulte Ver Registros del Sistema.

7 Ajustes de acción del relé

Cuando ocurre una decisión de acceso, el sistema activa el relé seleccionado. Use esta opción para integrar una baliza, una sirena o una cerradura auxiliar.



- **Port**: Seleccione el puerto del relé para activar. Obligatorio. No se pueden seleccionar los puertos de relé usados para cerraduras de puertas.
- **Open Time**: Configure cuánto tiempo mantener activo el relé. Mueva el control deslizante o ingrese un valor en el campo de entrada. Establezca de 1 a 120 segundos. Predeterminado: 3 segundos.
  - **Keep until event off**: Seleccione esta opción para mantener activo el relé hasta que termine el evento de control de acceso, sin importar el tiempo de apertura.
- **Contact Type**: Seleccione el tipo de contacto del relé. Obligatorio. Establezca esta opción después de seleccionar un puerto.
  - **Normal Open**: Normalmente abierto y se cierra cuando se activa el relé.
  - **Normal Close**: Normalmente cerrado y se abre cuando se activa el relé.
- **Schedule**: Seleccione un horario para activar el relé. Obligatorio. El valor predeterminado es **Always**.

Para guardar la configuración, haga clic en **Apply**.

> **Precaución**
>
> **Contact Type** es un ajuste aplicado al puerto del relé, no una regla. Al cambiar **Contact Type**, aparece un mensaje de confirmación. Haga clic en **OK** para aplicarlo de inmediato a todas las reglas y puertas que usan el puerto. Cambiar esto mientras el puerto está bloqueado o desbloqueado manualmente invierte la salida. Una puerta bloqueada puede abrirse.

8 Guardar regla

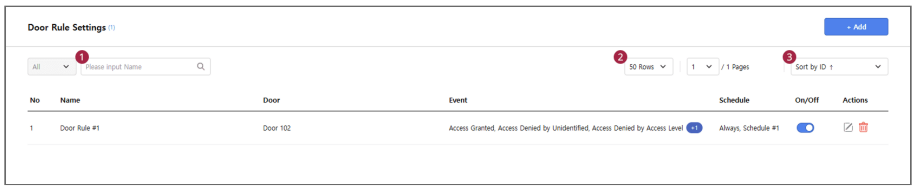
Después de completar todos los ajustes, haga clic en **Save** en la esquina superior derecha. El sistema agrega las reglas guardadas a la lista de reglas de puerta y las aplica de inmediato.



> **Información**
> Cree hasta 20 reglas de puerta.

Ver la lista de reglas de puerta

La lista de reglas de puerta muestra las reglas guardadas y el destino de cada regla.



- Ingrese el nombre de la regla de puerta en el campo de búsqueda (1) para encontrar una regla específica.
- Seleccione un valor en Filas (2) para cambiar el número de reglas por página.
- Para cambiar el criterio de ordenamiento, selecciona uno en **Sort by ID**(3).

En la lista de reglas de puerta aparecen los siguientes campos.

Ítem	Descripción
No	El número de la regla.
Name	El nombre de la regla.
Door	La puerta a la que se aplica la regla.
Event	El resultado de la decisión de acceso con una o más acciones habilitadas. Si existen varios resultados, la lista muestra solo parte de ellos.
Schedule	El horario aplicado a la regla.
On/Off	Activa o desactiva la regla.
Actions	Proporciona controles para editar ( ) o eliminar ( ) la regla.

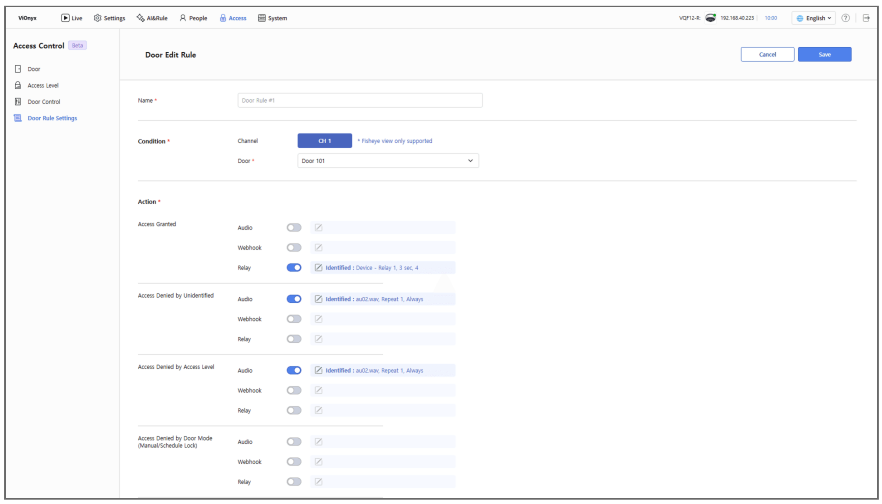
Habilitar/deshabilitar reglas de puerta

En la lista de reglas de puerta, haga clic en el interruptor de la columna **On/Off** para habilitar o deshabilitar la regla. Las reglas deshabilitadas no ejecutan acciones cuando ocurre un resultado de decisión de acceso. Use esto para pausar una regla sin eliminarla.



Editar regla de puerta

1. En la lista de reglas de puerta, haga clic en el botón al extremo derecho de la regla para editarla.
2. Cuando aparezca la pantalla **Edit Door Rule**, edite las condiciones y las acciones.



3. Para guardar los cambios, haz clic en **Save** en la esquina superior derecha de la pantalla.

Eliminar regla de puerta

En la lista de reglas de puerta, haga clic en el botón al extremo derecho de la regla para eliminarla. Cuando aparezca el mensaje de confirmación, haga clic en **OK**. Las reglas eliminadas no se pueden recuperar.

Configurar Sistema

Administra de forma sistemática la información del dispositivo, el firmware, el mantenimiento, las cuentas, el audio y los registros para operar eficazmente el sistema de cámaras. Revisa y actualiza periódicamente la información del dispositivo, el firmware, el mantenimiento, las cuentas, el audio y los registros para garantizar una operación estable y segura del sistema de cámaras.

Actualizar Información de la Cámara

Revise la información básica de la cámara e ingrese el nombre del dispositivo, la descripción y la ubicación para administrar varias cámaras de su organización.

Actualice la información de la cámara en las siguientes situaciones:

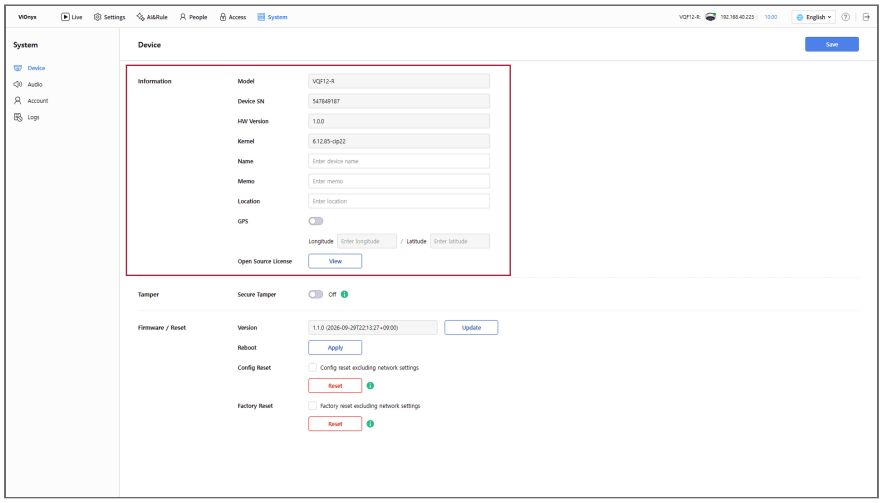
- Cambie el nombre de una cámara instalada por uno distintivo dentro de su organización.
- Agregue información adicional sobre la ubicación o el sitio de instalación de la cámara.
- Registre la ubicación precisa de la cámara ingresando coordenadas GPS.
- Agregue notas o descripciones específicas para cada cámara al administrar varias cámaras.

> **Información**
>
> - Los campos como el nombre del modelo, el número de serie y la versión de hardware son de solo lectura y no se pueden editar.
> - El nombre de la cámara, la nota y la ubicación admiten Unicode y aceptan coreano, inglés, números y caracteres especiales.

Revise la información básica de la cámara

Revise información básica como el modelo de la cámara, el número de serie y la versión de hardware.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Device** en la barra lateral izquierda.



Puede revisar la información básica a continuación en la sección **Information**. Estos campos son de solo lectura y no se pueden editar.

- **Model**: Modelo de la cámara
- **Device SN**: Número de serie de la cámara
- **HW Version**: Versión de hardware
- **Kernel**: Versión del kernel
- **Open Source License**: Haga clic en **View** para ver la información de la licencia de código abierto.

Establecer información de la cámara

Ingrese el nombre, la nota y la ubicación de la cámara para administrarlas de forma eficaz.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Device** en la barra lateral izquierda.

Ingrese el nombre

Ingrese un nombre personalizado para identificar la cámara con facilidad. Ingrese el nombre de la cámara en el campo **Name**.

- Hasta 64 caracteres.
- Admite coreano, inglés, números y caracteres especiales (`.` , `-` , `(` , `)`).

> *Ejemplo: "Entrada 1", "Sala de conferencias A"*

> **Información**
> El nombre de la cámara ingresado aparece en el menú del sistema y en toda la interfaz web, lo que facilita identificar la cámara.

Agregar nota

Ingrese información adicional o una nota para la cámara. Ingrese una nota o descripción en el campo **Memo**. Hasta 64

caracteres.

> *Ejemplo: departamento de instalación, nombre del administrador, fecha de instalación*

Ingrese información de ubicación

Ingrese la ubicación de instalación de la cámara como texto. Ingrese la ubicación de instalación de la cámara en el campo **Location**. Hasta 64 caracteres.

> *Ejemplo: "entrada del vestíbulo del primer piso", "área de espera de la sala de conferencias del segundo piso"*

Guardar ajustes

Después de ingresar toda la información, haga clic en **Save** en la esquina superior derecha de la pantalla.

Establecer coordenadas GPS

Ingrese la ubicación geográfica exacta de la cámara como coordenadas GPS.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Device** en la barra lateral izquierda.
3. Para habilitar el ajuste de GPS, haga clic en el interruptor **GPS** en la sección **Information**.



4. Ingrese la información de longitud y latitud.

   > *Ejemplo: Seúl (37.5665, 126.9780)*

5. Haga clic en **Save** en la esquina superior derecha de la pantalla para guardar el ajuste.

> **Información**
>
> - Ingrese las coordenadas GPS en formato de grados decimales (DD).
> - Para deshabilitar el ajuste de GPS, haga clic de nuevo en el interruptor **GPS**.

Actualizar Firmware

Esta función actualiza el firmware de la cámara a la versión más reciente. Las actualizaciones de firmware incorporan nuevas funciones, mejoras de rendimiento y parches de seguridad.

Actualice el firmware en las siguientes situaciones.

- Para usar nuevas funciones
- Para aplicar parches de seguridad y proteger la cámara
- Para mejorar el rendimiento de la cámara

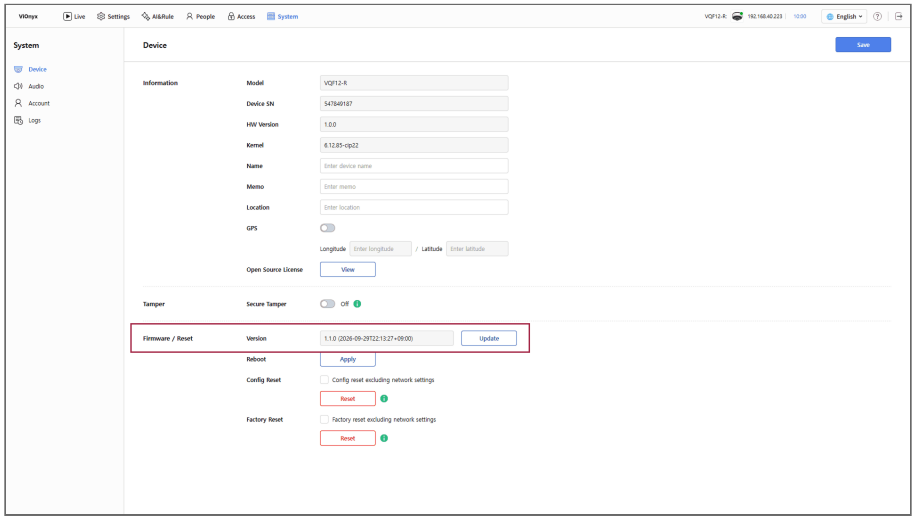
- Cuando el soporte técnico recomienda una versión específica de firmware

> **Información**
>
> - La cámara se reinicia durante una actualización de firmware y no está disponible durante ese tiempo.
> - Asegúrese de que el dispositivo tenga suficiente energía antes de iniciar la actualización de firmware.
> - Use solo archivos de firmware oficiales (.bin) proporcionados por el soporte técnico de Suprema.

Verificar la versión actual de firmware

Verifique la versión de firmware instalada de la cámara.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Device** en la barra lateral izquierda.

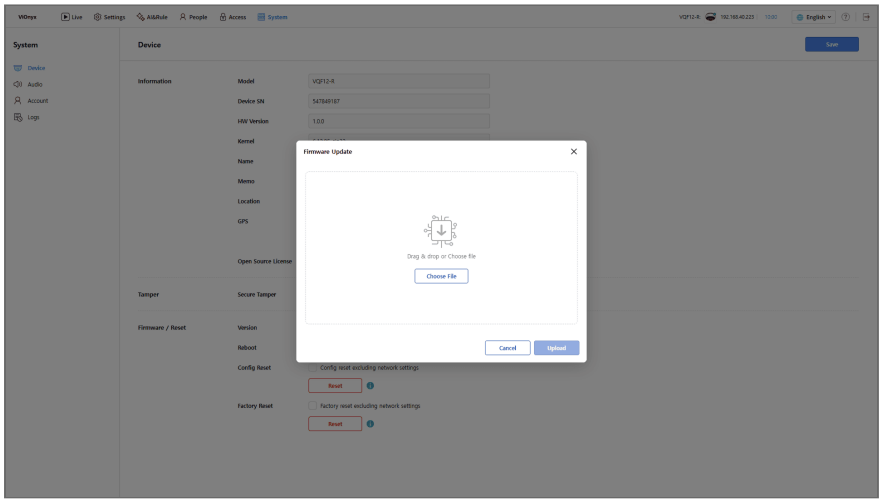


En la sección **Firmware / Reset**, verifique la versión de firmware instalada actualmente en **Version**.

Actualizar firmware

Seleccione el nuevo archivo de firmware para actualizar el dispositivo.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Device** en la barra lateral izquierda.
3. En la sección **Firmware / Reset**, haga clic en **Update**.
4. Cuando aparezca la ventana emergente **Firmware Update**, seleccione el archivo de firmware (.bin) proporcionado por Suprema.



- La extensión del archivo debe ser .bin.
- Arrastre el archivo al área de carga o haga clic en **Choose File** para seleccionar el archivo.

5. Después de seleccionar un archivo, **Upload** se activa.
6. Haga clic en **Upload** para iniciar la actualización de firmware.
7. Después de que termine la carga, aparece una ventana emergente de confirmación de reinicio. Haga clic en **OK** para reiniciar la cámara y completar la actualización de firmware.

- Vuelva a conectarse a la interfaz web después de que la cámara se reinicie. Para verificar la nueva versión de firmware, vaya a **Device**.
- No puede cancelar la actualización de firmware una vez que inicia. Espere hasta que termine la actualización.

Mantener la Cámara

Gestiona la cámara de forma eficaz reiniciándola o inicializando la configuración. Cubre tres métodos: reinicio, restablecimiento de la configuración y restablecimiento de fábrica.

Usa la función de mantenimiento de la cámara en las siguientes situaciones.

- Cuando una persona externa que no es administradora intenta quitar la cubierta de la cámara y necesitas aplicar medidas de seguridad para que la cámara deje de operar normalmente.
- Después de cambiar la configuración de red, para aplicar la nueva configuración.
- Cuando la cámara responde lentamente o su rendimiento disminuye.
- Cuando el sistema no funciona normalmente.
- Cuando necesitas restaurar todas las configuraciones de la cámara a los valores predeterminados.
- Antes de entregar la cámara a otro usuario, para eliminar toda la información.
- Cuando un problema del sistema requiere restaurar los valores predeterminados de fábrica.

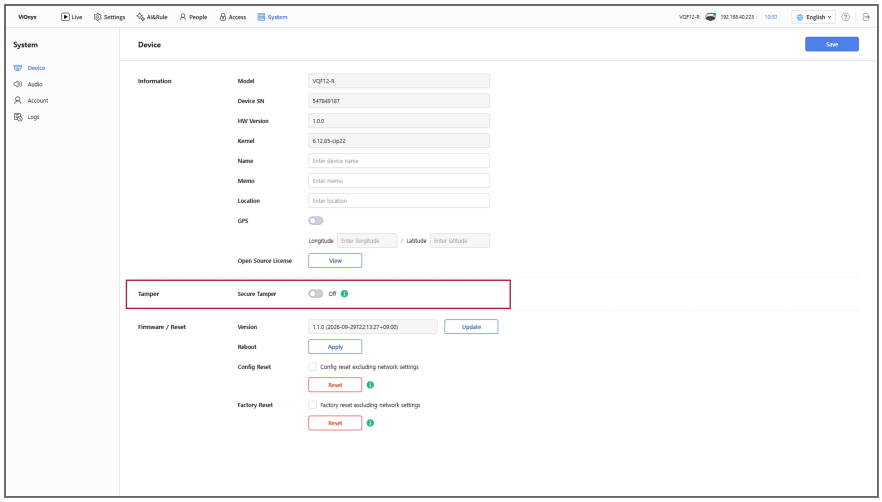
Alerta

- No apagues la cámara durante el reinicio o la inicialización.
- **El restablecimiento de fábrica** elimina de forma permanente todos los datos del usuario, los registros de eventos y los registros. Esta acción no se puede revertir; procede con extrema precaución.
- Haz una copia de seguridad de los datos necesarios antes de inicializar.

Tamper

Activa la función **Tamper** de la cámara para eliminar los certificados y las claves de la cámara cuando una persona externa que no es administradora intenta quitar la cubierta de la cámara, lo que evita que la cámara funcione normalmente.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Device** en la barra lateral izquierda.
3. Haz clic en el interruptor de la sección **Tamper** para activar la función.



4. Cuando aparezca el mensaje de advertencia, haga clic en **OK**.

Esta función guarda los cambios automáticamente sin hacer clic en **Save**.

Precaución

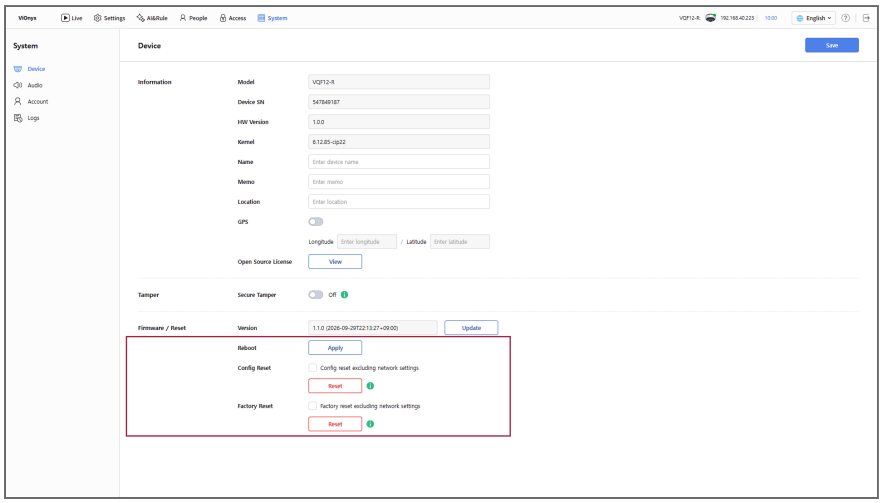
Cuando la función **Tamper** está activada y el administrador debe quitar la cubierta de la cámara para mantenimiento, desactiva temporalmente la función **Tamper** antes de continuar. Vuelve a activarla después de completar la tarea para mantener la seguridad.

Reiniciar la cámara

Reinicia la cámara para aplicar cambios de configuración o restaurar el rendimiento del sistema. El reinicio reinicializa el sistema y mantiene la configuración actual.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Device** en la barra lateral izquierda.

3. En la sección **Firmware / Reset**, debajo de **Reboot**, haz clic en **Apply**.



4. Cuando aparezca la ventana emergente de confirmación del reinicio, haz clic en **OK**.

Información

- Mientras se reinicia, la cámara no está disponible temporalmente. El reinicio tarda al menos 1 a 2 minutos.
- No apagues la cámara durante el reinicio. Puede producirse daño en el sistema.
- Si la dirección IP de la cámara cambia después del reinicio, conéctate con la nueva dirección IP.
- Cuando comienza el reinicio, la conexión de la interfaz web se desconecta automáticamente. Este comportamiento es normal.

Restablecimiento

Inicializa la configuración de la cámara o restáurala por completo a los valores predeterminados de fábrica. Hay dos métodos de inicialización disponibles; eliminan datos distintos, así que elige con cuidado.

Comparación de métodos de inicialización

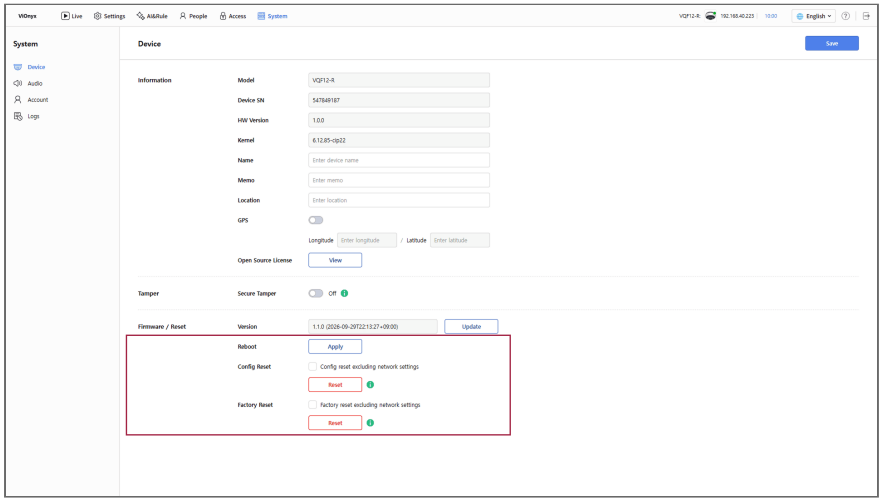
Método	Descripción	Datos eliminados	Datos conservados
Config Reset	Inicializar solo la configuración	Configuración de la cámara, configuración de red (opcional), perfiles de video, reglas, cuentas	Información del usuario, datos faciales, eventos/registros
Factory Reset	Eliminar todos los datos y restaurar los valores predeterminados de fábrica	Todas las configuraciones, información del usuario, eventos, registros, cuentas	-

Config Reset

Inicializa solo la configuración; conserva la información del usuario y los datos de registros.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.

2. Haz clic en **Device** en la barra lateral izquierda.
3. En la sección **Firmware / Reset**, debajo de **Config Reset**, haz clic en **Reset**.



Para excluir la configuración de red de la inicialización, haz clic en la casilla de verificación de la opción **Config reset excluding network settings**.

4. Cuando aparezca la ventana emergente de confirmación del restablecimiento de la configuración, haz clic en **OK**.

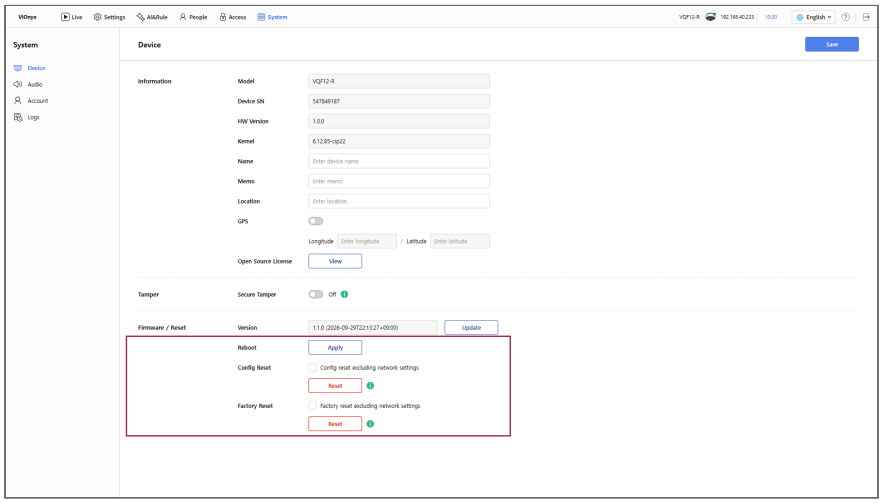
El restablecimiento de la configuración continúa y la cámara se reinicia automáticamente.

Factory Reset

Inicializa por completo la cámara para restaurarla a los valores predeterminados de fábrica. Esta acción no se puede deshacer.

> **Alerta**
>
> El restablecimiento de fábrica elimina por completo todos los datos. Esta acción no se puede revertir; procede con extrema precaución.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Device** en la barra lateral izquierda.
3. En la sección **Firmware / Reset**, debajo de **Factory Reset**, haz clic en **Reset**.



Para excluir la configuración de red de la inicialización, haz clic en la casilla de verificación de la opción **Config reset excluding network settings**.

4. Cuando aparezca la ventana emergente de confirmación del restablecimiento de fábrica, haz clic en **OK**.
5. Cuando aparezca la ventana emergente de confirmación final, ingresa la contraseña de administrador.
6. Haga clic en **OK**.

> **Información**
>
> - Después de completar el restablecimiento de fábrica, los siguientes elementos se restauran a sus valores predeterminados.
>   - ID de administrador: **admin**
>   - Configuración de red: DHCP
>   - Todos los datos del usuario, eventos y registros: eliminados
> - Después del restablecimiento de fábrica, establece una nueva contraseña predeterminada al acceder a la interfaz web.

Subir Clips de Audio

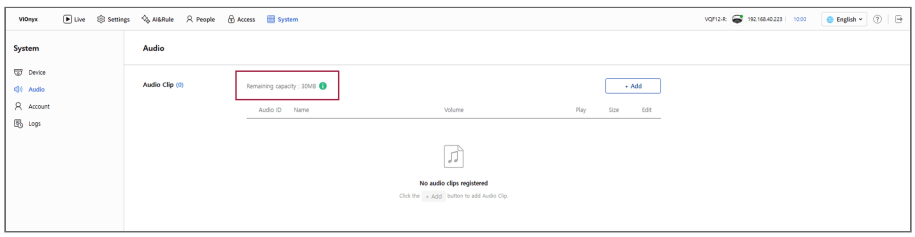
Sube clips de audio para la cámara y aplícalos como tonos de alarma o indicaciones de voz. Sube y administra archivos de audio en formato WAV.

Sube clips de audio en las siguientes situaciones.

- Cuando necesites subir tonos de alarma para que suenen cuando ocurra un evento
- Cuando necesites agregar indicaciones de voz en varios idiomas
- Cuando necesites agregar mensajes de voz para situaciones específicas

Verificar capacidad de almacenamiento de audio

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Audio** en la barra lateral izquierda.
3. Puedes verificar la capacidad restante del almacenamiento de audio en la sección **Audio Clip**.



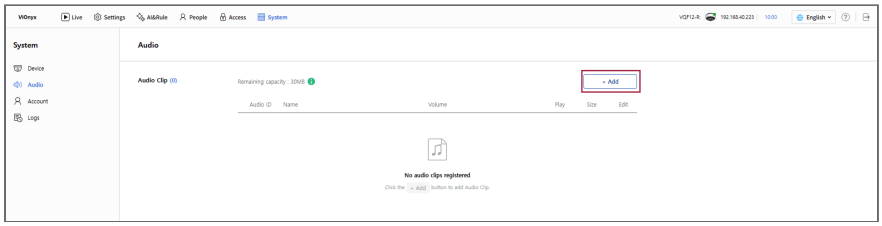
Preparar archivos de audio

Antes de subir clips de audio, verifica lo siguiente.

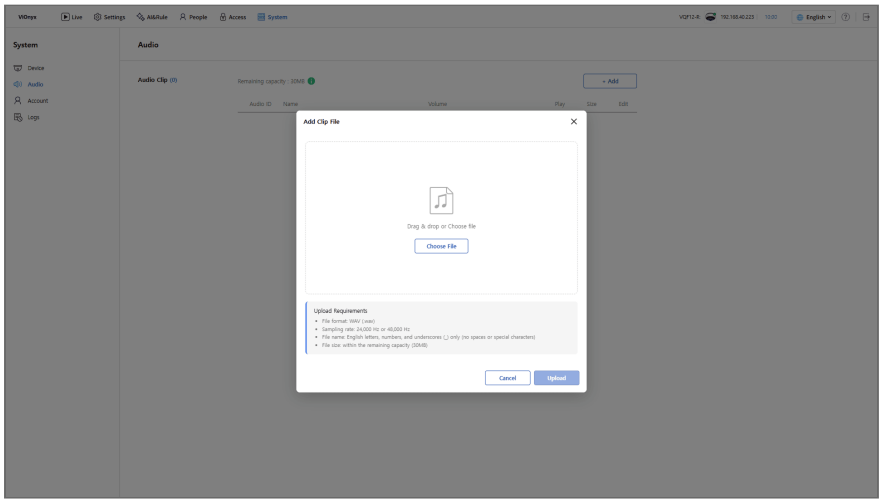
- **Formato de archivo**: Solo se admite la extensión `.wav`.
- **Frecuencia de muestreo**: Usa una frecuencia de muestreo de 48 kHz o superior.
- **Nombre de archivo**: Usa solo letras, números y guiones bajos (`_`) en inglés, hasta 64 caracteres. No se permiten espacios ni caracteres especiales.
- **Tamaño de archivo**: Puedes subir archivos dentro de la capacidad restante.

Subir clips de audio

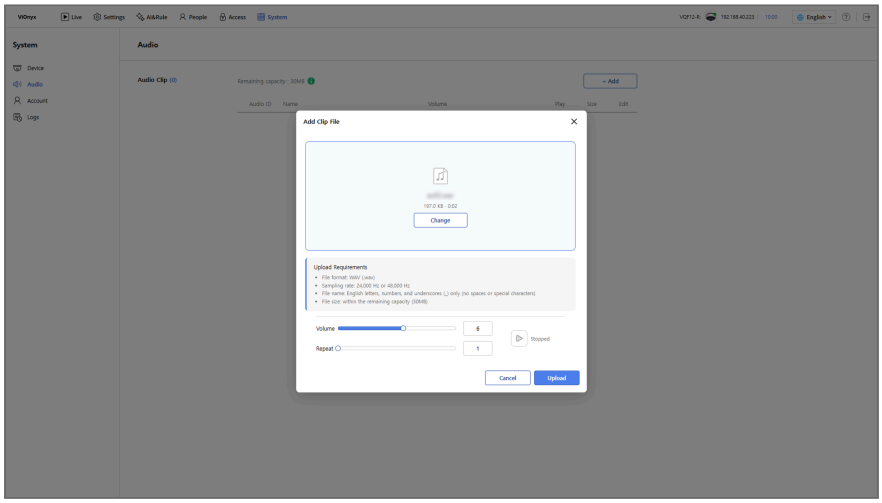
1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Audio** en la barra lateral izquierda.
3. Haga clic en **+ Add** en la esquina superior derecha de la pantalla.



4. Aparece la ventana emergente **Add Clip File**.



5. Arrastra y suelta un archivo WAV en el área de carga, o haz clic en **Choose File** y selecciona un archivo WAV almacenado localmente.
6. Después de completar la carga, ajusta las opciones de volumen y repetición.



7. Haz clic en **Upload** para subir el clip de audio.

Consulta los clips de audio subidos en la lista.



Información

- Ajusta el control deslizante de volumen para definir el volumen de reproducción del clip de audio.
- Para reproducir el clip de audio, haz clic en ▶.

Eliminar clip de audio

Haz clic en a la derecha del clip de audio que quieres eliminar.



Información

- Si el clip de audio que quieres eliminar está aplicado a una regla de IA, se excluye automáticamente de la configuración de la regla de IA.
- Para obtener más información sobre la configuración de la regla de IA, consulta Ajustes de Reglas de IA.

Actualizar Contraseña de la Cuenta de Administrador

Cambie la contraseña de la cuenta de administrador para mejorar la seguridad de acceso a la cámara. Cambie la

contraseña periódicamente como buena práctica de seguridad.

Cambie la contraseña en las siguientes situaciones.

- Al configurar la cuenta de administrador por primera vez para mejorar la seguridad
- Al renovar la contraseña para cumplir con la política de seguridad rutinaria
- Si la contraseña se compromete y requiere un cambio inmediato
- Al reemplazar al administrador, establezca una nueva contraseña

Revisar reglas de la contraseña

Revise las siguientes reglas antes de establecer la contraseña. Todas las reglas deben cumplirse.

- La contraseña debe tener al menos 12 caracteres. Longitud máxima: 64 caracteres.
- Incluya al menos una letra minúscula (`a-z`) y una mayúscula (`A-Z`).
- Incluya al menos un dígito (`0-9`) y un carácter especial.

  > *Ejemplos de caracteres especiales:* `"` `!` `@` `#` `$` `%` `^` `&` `*` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}`

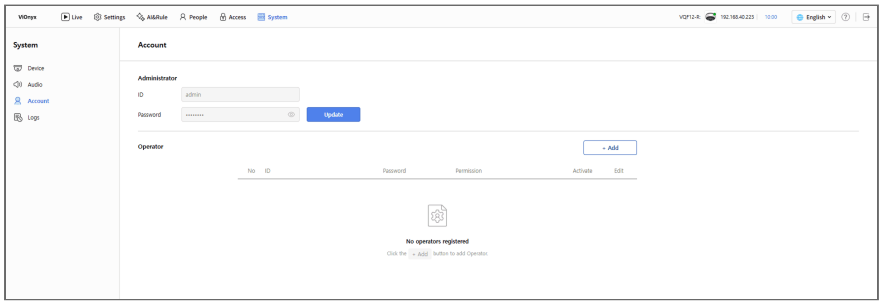
- No incluya secuencias de 4 o más caracteres consecutivos (por ejemplo, `1234` , `abcd`) ni 4 o más caracteres idénticos.
- El nombre de usuario (sin distinguir mayúsculas y minúsculas) no debe incluirse en la contraseña.

  > *admin, Admin, ADMIN, Admin123! etc.*

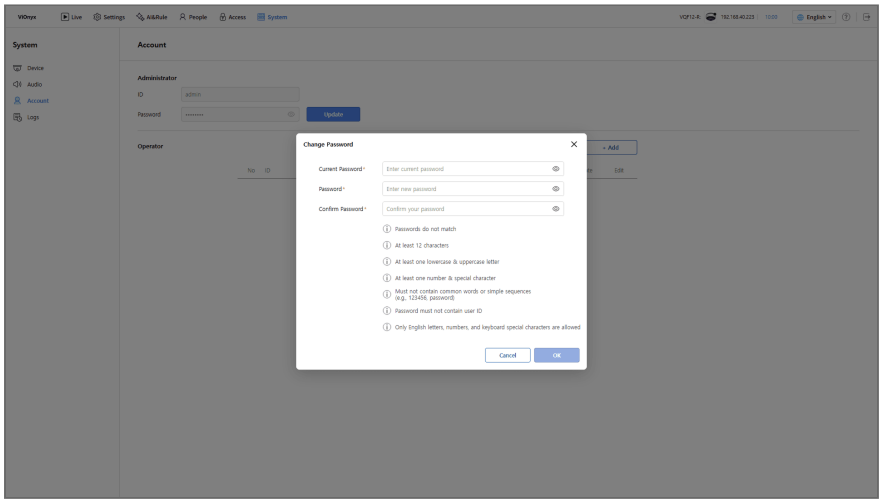
- No se permiten contraseñas débiles comunes como `password` , `qwerty` , `123456` .
- Use solo letras del alfabeto inglés, números y caracteres especiales de un teclado con distribución en inglés.

Cambiar contraseña de administrador

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Account** en la barra lateral izquierda.



3. En la sección **Administrator**, haga clic en **Update**.
4. Cuando aparezca la ventana **Change Password**, ingrese la contraseña actual de administrador en el campo **Current Password**.



5. Ingrese la nueva contraseña en los campos **Password** y **Confirm Password**, en ese orden.
6. Haga clic en **OK** para cambiar la nueva contraseña.

Cuando aparezca el mensaje de éxito, el cambio de contraseña estará completo.

> **Información**
>
> - Después de cambiar la contraseña, es posible que deba iniciar sesión de nuevo.
> - Los eventos de cambio de contraseña se registran en el registro del sistema.

Si olvida la contraseña

Recupere una contraseña de administrador perdida con los siguientes métodos.

- **Restablecimiento de fábrica**: ejecutar un restablecimiento de fábrica restaura la cuenta de administrador a los valores predeterminados. Advertencia: el restablecimiento de fábrica elimina todos los datos. Para obtener más información sobre la inicialización de fábrica, consulte la Guía de instalación de ViOnyx.
- **Contactar al soporte técnico**: contacte a Equipo de Soporte Técnico global de Suprema para obtener ayuda.

Administrar Operadores

Además de los administradores, agregue, edite o elimine cuentas de operador con permisos limitados. Los operadores pueden administrar ciertas funciones de la cámara en nombre de los administradores.

Además, agregue una cuenta solo para ONVIF que el NVR/VMS usa para la autenticación de ONVIF y RTSP. Una cuenta solo para ONVIF es obligatoria para habilitar la conmutación por error del Perfil S de ONVIF.

Agregue operadores en las siguientes situaciones.

- Asigne personal adicional para operar la cámara.
- Otorgue solo permisos específicos.
- Cuando varias personas deben colaborar para administrar la cámara.
- Otorgue a los miembros del equipo permisos de solo lectura o de edición.

Información

- Agregue hasta 10 operadores.
- Los operadores no pueden agregar otros operadores. Solo los administradores pueden agregar operadores.
- Las contraseñas de los operadores siguen las mismas reglas que las contraseñas de los administradores. Para obtener más información, consulte Actualizar Contraseña de la Cuenta de Administrador.
- Cada operador solo puede cambiar la información de su propia cuenta.

Tipos de permisos de operador

Seleccione uno de los siguientes 3 permisos al agregar un operador.

- **Read Only**: Ve todas las configuraciones y registros de la cámara; no puede cambiar la configuración.
- **Read Write**: Acceda a todos los menús excepto el menú Administrador y cambie los ajustes de la cámara. Los operadores pueden cambiar su propia contraseña, pero no la de otros operadores ni la de los administradores.
- **ONVIF Only**: Una cuenta exclusiva del dispositivo que el NVR/VMS usa para la autenticación de ONVIF y RTSP. No es posible iniciar sesión en la interfaz web. Obligatoria al habilitar la conmutación por error del Perfil S de ONVIF. Para obtener más información, consulte Configurar Ajustes de Red.

Limitaciones de las cuentas solo para ONVIF

Las cuentas solo para ONVIF tienen las siguientes limitaciones, a diferencia de las cuentas de operador estándar.

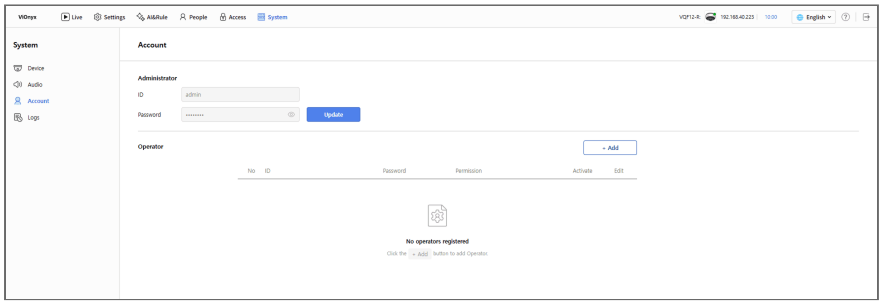
- Cree solo una por dispositivo.
- Después de crear la cuenta, el sistema bloquea los cambios de ID, contraseña y permisos. Solo habilite, deshabilite o elimine la cuenta.
- Deshabilitar la cuenta impide la conmutación por error del Perfil S.
- Cuando la conmutación por error del Perfil S está habilitada, el sistema bloquea la eliminación de la cuenta. Primero, cambie el modo ONVIF a **Profile T Only**.

Precaución

Las cuentas solo para ONVIF no permiten cambiar el ID ni la contraseña después de crearlas. Decida con anticipación qué ingresar en el NVR/VMS y almacene la información de la cuenta de forma segura. Para cambiar la contraseña, elimine la cuenta y créela de nuevo.

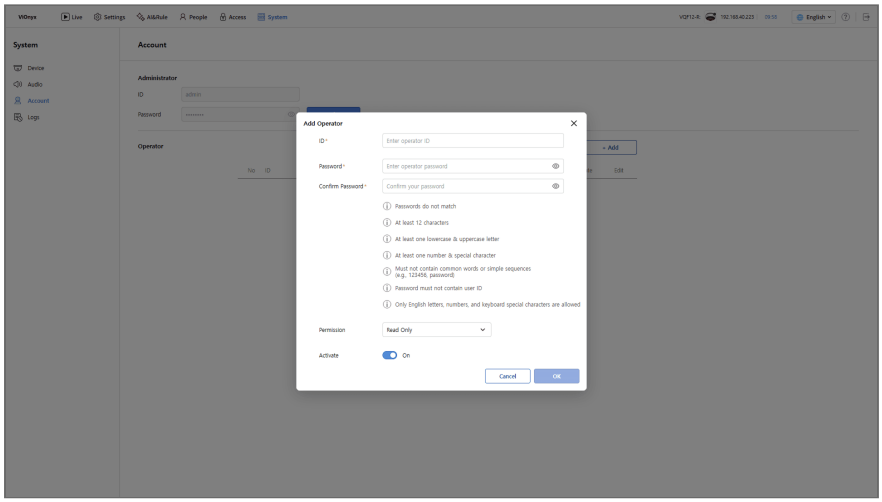
Agregar operador

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Account** en la barra lateral izquierda.



3. En la sección **Operator**, haga clic en **+ Add**.

4. Cuando aparezca la ventana emergente **Add Operator**, ingrese la información requerida.



- **ID**: Ingrese el ID único del operador.
  - Hasta 64 caracteres.
  - Puede incluir letras coreanas, letras inglesas y números.
  - Caracteres especiales permitidos: `_`, `.`, `-`, `(`, `)`.
  - Debe ser único y no duplicarse con otro operador.
- **Password**: Ingrese la contraseña del operador. Sigue las mismas reglas que la contraseña del administrador. Para obtener más información, consulte Actualizar Contraseña de la Cuenta de Administrador.
- **Confirm Password**: Vuelva a ingresar la contraseña.
- **Permission**: Seleccione el permiso del operador. Seleccione **ONVIF Only** para crear una cuenta solo para ONVIF.
- **Enabled**: Active o desactive la cuenta del operador.

5. Después de ingresar toda la información, haga clic en **OK**.

Después de agregar un nuevo operador, la nueva cuenta aparece en la lista.

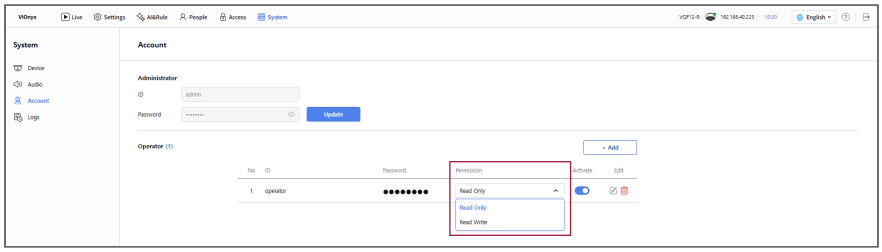
Información

- Después de agregar un operador, inicie sesión con esa cuenta para verificar que los permisos se apliquen correctamente.
- Entregue de forma segura al operador su ID y contraseña.

Cambiar permisos del operador

Cambie los permisos de un operador.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Account** en la barra lateral izquierda.
3. En la sección **Operator**, haga clic en el campo **Permission** del operador cuyos permisos desea cambiar.

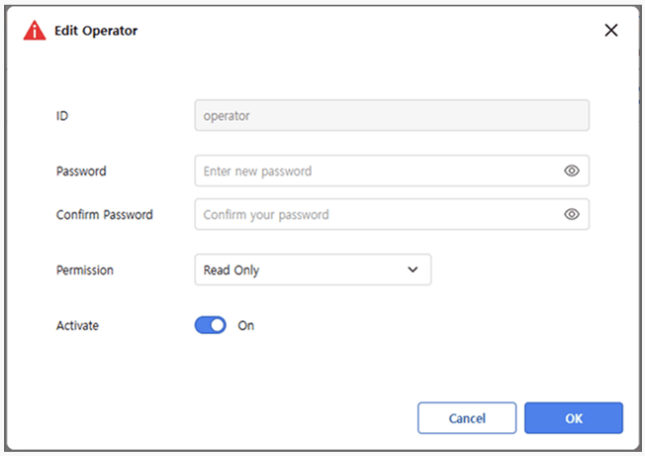


4. Seleccione los permisos deseados de la lista.

Cuando el cambio de permisos se completa correctamente, aparece un mensaje de éxito en la esquina superior derecha de la pantalla.

Consejo

Haga clic en para abrir la ventana **Edit Operator**. En el campo **Permission**, cambie a los permisos deseados y luego haga clic en **OK**.



Información

Las cuentas solo para ONVIF no permiten cambios de permisos. Si requiere otro permiso, agregue una nueva cuenta de operador.

Deshabilitar operador

Desactive temporalmente la cuenta de un operador. Bloquea el acceso sin eliminar la cuenta.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Account** en la barra lateral izquierda.

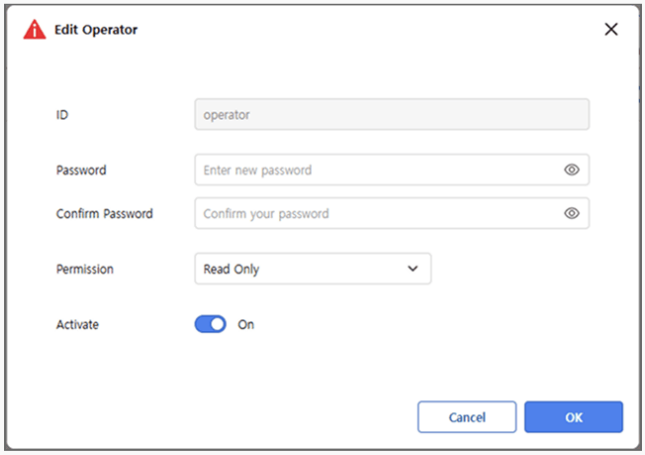
3. En la sección **Operator**, haga clic en el interruptor del campo **Enabled** del operador que desea desactivar.



Cuando la desactivación se completa correctamente, aparece un mensaje de éxito en la esquina superior derecha de la pantalla. Las cuentas de operador deshabilitadas no pueden iniciar sesión.

Consejo

Haga clic en para abrir la ventana **Edit Operator**. Haga clic en el interruptor del campo **Enabled** para desactivar la cuenta. Haga clic en **OK** para guardar los cambios.



Información

Las cuentas deshabilitadas se pueden reactivar más tarde.

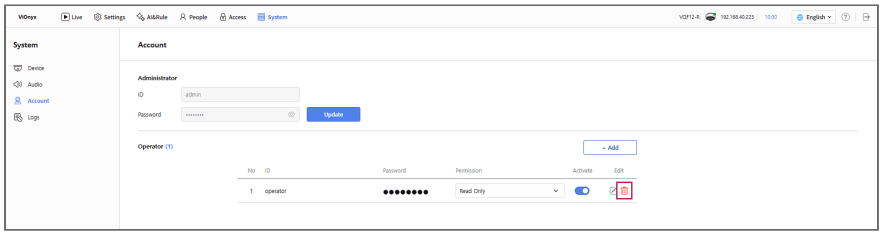
Precaución

Si un operador ya inició sesión, se le denegará el acceso en el siguiente intento de inicio de sesión.

Eliminar operador

Puede eliminar permanentemente las cuentas de operador. Las cuentas eliminadas no se pueden recuperar.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Account** en la barra lateral izquierda.
3. En la sección **Operator**, haga clic en del operador que desea eliminar.



4. Cuando aparezca el mensaje de advertencia, haga clic en **OK**.

Cuando la eliminación se completa correctamente, aparece un mensaje de éxito en la esquina superior derecha de la pantalla. La cuenta de operador se quita de la lista.

> **Información**
>
> Si **Profile T priority / S fallback** está habilitado, el sistema bloquea la eliminación de la cuenta solo para ONVIF. Vaya a **Settings** → **Network** → **Network**, cambie el modo ONVIF a **Profile T Only** y vuelva a intentarlo. Para obtener más información, consulte Configurar Ajustes de Red.

Ver Registros del Sistema

Ve y administra registros de acceso de usuarios a la cámara, eventos, análisis de IA y operaciones del sistema. En la interfaz web, filtra los registros por categoría, nivel y actor. Exporta los registros a CSV o descarga los registros cifrados del dispositivo para un análisis detallado.

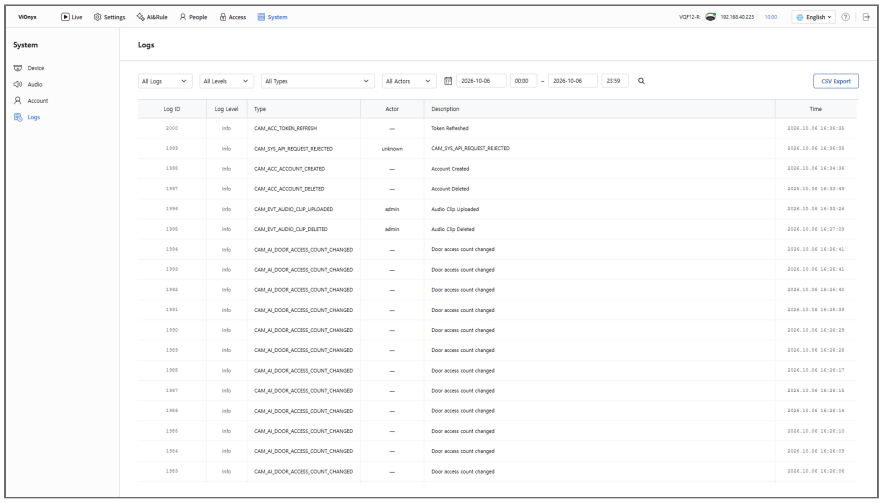
Revise los registros en las siguientes situaciones.

- Para verificar quién accedió a la cámara y cuándo
- Para rastrear cuándo ocurrió un evento específico
- Para revisar operaciones importantes del sistema, como el arranque y el reinicio
- Para revisar los registros de acceso con fines de monitoreo de seguridad
- Para recopilar registros del sistema para la solución de problemas
- Cuando necesites distinguir las acciones de un administrador u operador de las acciones automáticas de la cámara

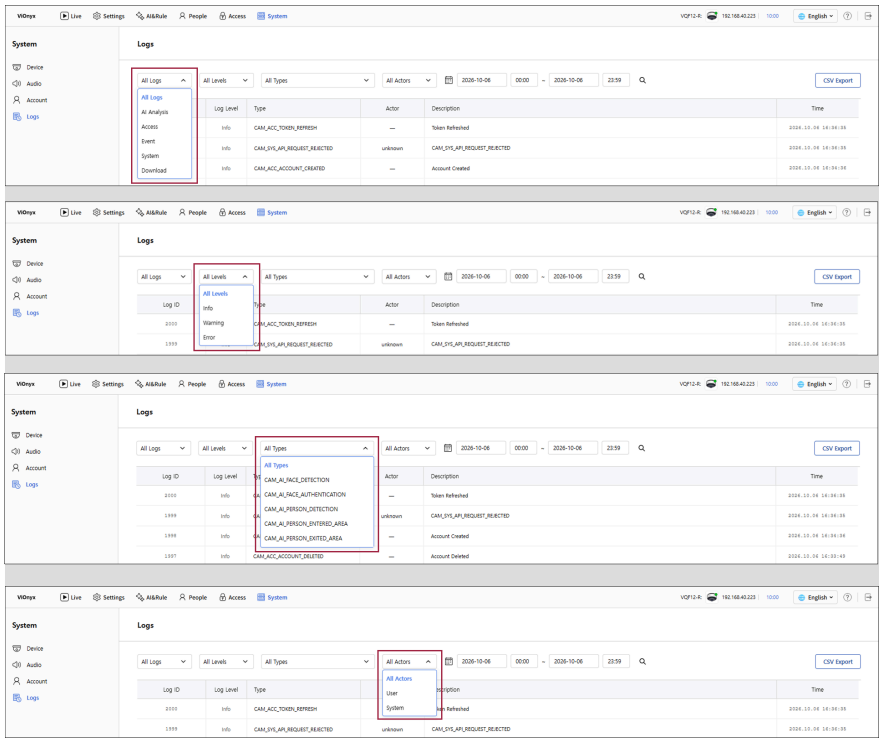
> **Información**
>
> - Los registros se conservan automáticamente según el tamaño de memoria del dispositivo.
> - Cada tipo de registro se conserva durante aproximadamente 1 mes.
> - Cuando la memoria se llena, los registros más antiguos se eliminan automáticamente.
> - Solo los administradores y los operadores con permiso de lectura y escritura pueden usar el menú **Logs**. Sin embargo, solo los administradores pueden ver los registros de **System**.

Ver registros

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Logs** en la barra lateral izquierda. Ver todos los registros.



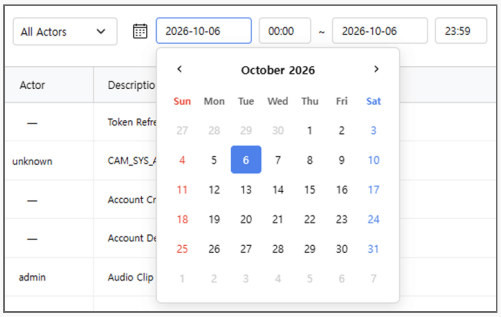
3. Selecciona criterios en **All Logs**, **All Levels**, **All Types** y **All Actors** en la parte superior izquierda de la lista de registros. Úsalos para filtrar los registros por categoría, nivel, tipo y actor.



4. Haga clic en 🔍 en la parte superior de la lista de registros para filtrar los registros según los criterios seleccionados.

Información

- Para ver los registros de un período específico, haga clic en los campos de entrada de fecha y hora. Cuando aparezcan el calendario y el selector de hora, seleccione la fecha y hora de inicio deseadas. Establezca la fecha y hora de fin del mismo modo.



- Desplácese hacia abajo en la lista para actualizarla y seguir viendo registros anteriores.
- Para obtener más información sobre los tipos de registro, consulte Tipos de Registros del Sistema.

Tipos de registro

Los registros se clasifican de la siguiente manera.

- **AI Analysis**: Ver registros de eventos relacionados con el análisis de IA.
- **Access**: Consulta los registros relacionados con el acceso de usuarios y las cuentas, como inicio de sesión, cierre de sesión y creación de cuentas.
- **Event**: Registros de eventos, envíos de webhook y ejecuciones de reglas.
- **System**: Registros de operaciones del sistema, como arranque, reinicio e inicialización. Este registro **solo lo pueden ver los administradores**.

Información

Seleccione **Download** para descargar el archivo de registro cifrado del dispositivo. Para más información, consulte Descarga de registros del dispositivo.

Niveles de registro

Los registros se clasifican en los siguientes niveles.

- **Info**: Ver registros de mensajes informativos generales.
- **Warning**: Ver registros de mensajes de advertencia.
- **Error**: Ver registros de mensajes de error.

Actores

La entidad que genera un registro se llama actor. Los actores se clasifican de la siguiente manera.

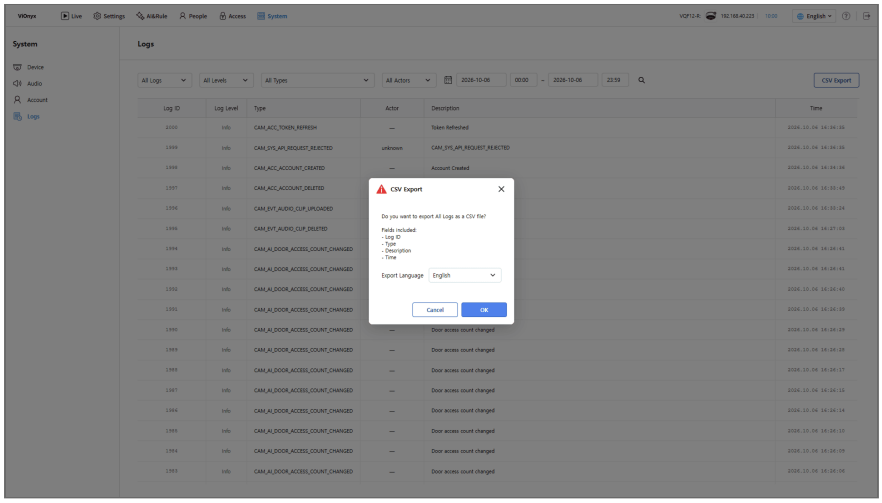
- **User**: Un administrador u operador que ejecuta tareas directamente en la interfaz web.

- **System**: Una cámara que ejecuta tareas automáticamente según reglas de IA y horarios.

Exportar registros

Descargue los registros en formato CSV para su análisis externo o archivo.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Logs** en la barra lateral izquierda.
3. Selecciona criterios para los registros que se exportarán en **All Logs**, **All Levels**, **All Types** y **All Actors** en la parte superior izquierda de la lista de registros. Establezca un período de búsqueda para exportar registros de un rango de tiempo específico. El archivo CSV refleja los criterios y el período seleccionados.
4. Haga clic en **CSV Export** en la parte superior derecha de la pantalla.
5. Cuando aparezca la ventana emergente **CSV Export**, seleccione el idioma de exportación.



6. Haga clic en **OK**.

Descargue la lista de registros como archivo CSV.

Información

- Formato del nombre de archivo CSV: `system-logs-YYYYMMDD_HHMMSS.csv`.

  > *Ejemplo: system-logs-20240326_153000.csv*

- El archivo se guarda en la carpeta de descargas predeterminada del navegador o en una ubicación seleccionada por el usuario.

Retención y administración de registros

Eliminación automática de registros

Cuando la memoria de la cámara se llena, los registros más antiguos se eliminan automáticamente.

Categoría de registro	Período de retención
AI Analysis	Aproximadamente un mes
Access	Aproximadamente un mes
Event	Aproximadamente un mes
System	Aproximadamente un mes

Cómo conservar registros importantes

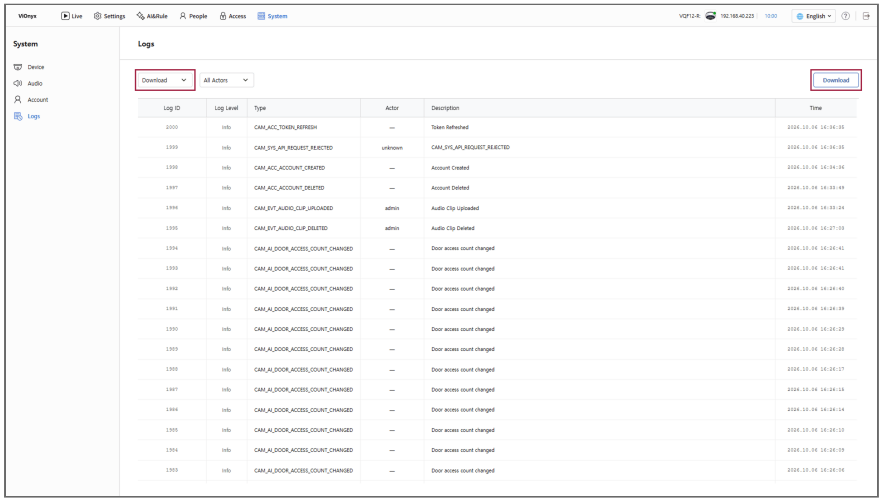
Para conservar registros importantes a largo plazo, siga estos pasos:

- Exporte los registros a CSV con regularidad.
- Guarde los archivos exportados en almacenamiento externo (NAS, almacenamiento en la nube, etc.).
- Incluya la fecha de exportación y el período del registro en el archivo.

Descarga de registros del dispositivo

Descargue los archivos de registro almacenados en el dispositivo en formato cifrado. Los registros del dispositivo son archivos de registro detallados que incluyen todos los eventos y registros operativos generados por el sistema de la cámara. El archivo está cifrado para mantenerlo seguro y entréguelo a Equipo de Soporte Técnico global de Suprema cuando sea necesario para la solución de problemas.

1. Haga clic en el menú **System** en la esquina superior izquierda de la pantalla.
2. Haz clic en **Logs** en la barra lateral izquierda.
3. Seleccione **Download** en **All Logs** en la parte superior izquierda de la lista de registros.



4. Para descargar registros de un actor específico, selecciona un actor en **All Actors**. Si no seleccionas ningún actor, el sistema descarga los registros de todos los actores. Para obtener más información sobre los actores, consulta Actores.
5. Haga clic en **Download** en la parte superior derecha de la lista de registros.

Descargue localmente el archivo de registro del dispositivo. El nombre de archivo usa el formato `device_logs_{device-serial-`

number}_YYYYMMDDTHHMMSS.zip.enc .

> *Ejemplo: device_logs_1234567890_20240326T153000.zip.enc*

Tipos de Registros del Sistema

Proporciona información sobre los tipos de registros disponibles en los registros del sistema.

Tipos de registro	Descripción
CAM_AI_FACE_DETECTION	**Face Detection**
CAM_AI_FACE_AUTHENTICATION	**Face Authentication**
CAM_AI_PERSON_DETECTION	**Person Detection**
CAM_AI_PERSON_ENTERED_AREA	**Person Entered Area**
CAM_AI_PERSON_EXITED_AREA	**Person Exited Area**
CAM_AI_INTRUSION_ENTRY_AREA_APPEARED	**Intrusion Detected (Entry Area)**
CAM_AI_INTRUSION_EXIT_AREA_APPEARED	**Intrusion Detected (Exit Area)**
CAM_AI_PEOPLE_COUNT_CHANGED	**People Count Changed**
CAM_AI_PEOPLE_COUNT_LIMIT_REACHED	**People Count Limit Reached**
CAM_AI_LINE_CROSSED	**Line Crossed**
CAM_AI_FACE_AUTHENTICATION_FAILED	**Face Authentication Failed**
CAM_AI_DOOR_ACCESS_EVENT_OFF	**Door access event off**
CAM_AI_DOOR_ACCESS_SOURCE	**Door access source signal**
CAM_AI_DOOR_ACCESS_AREA_ENTERED	**Door access area entered**
CAM_AI_DOOR_ACCESS_AREA_EXITED	**Door access area exited**
CAM_AI_DOOR_ACCESS_LINE_CROSSED	**Door line crossed**
CAM_AI_DOOR_ACCESS_COUNT_CHANGED	**Door access count changed**
CAM_EVT_RULE_TRIGGERED	**Rule Triggered**
CAM_EVT_RULE_CREATED	**Rule Created**

Tipos de registro	Descripción
CAM_EVT_RULE_UPDATED	**Rule Updated**
CAM_EVT_RULE_DELETED	**Rule Deleted**
CAM_EVT_RULE_ENABLED	**Rule Enabled**
CAM_EVT_RULE_DISABLED	**Rule Disabled**
CAM_EVT_RULE_USERS_ADDED	**Rule users added**
CAM_EVT_RULE_USERS_REMOVED	**Rule users removed**
CAM_EVT_RULE_RELAY_SCHEDULE_BLOCKED	**Relay denied — outside scheduled hours**
CAM_EVT_WEBHOOK_SEND	**Webhook Send Attempt**
CAM_EVT_WEBHOOK_SENT	**Webhook Sent**
CAM_EVT_WEBHOOK_FAILED	**Webhook Failed**
CAM_EVT_WEBHOOK_CREATED	**Webhook Created**
CAM_EVT_WEBHOOK_UPDATED	**Webhook Updated**
CAM_EVT_WEBHOOK_DELETED	**Webhook Deleted**
CAM_EVT_FACE_USER_CREATED	**Face User Created**
CAM_EVT_FACE_USER_UPDATED	**Face User Updated**
CAM_EVT_FACE_USER_DELETED	**Face User Deleted**
CAM_EVT_FACE_USER_CREATE_FAILED	**Face User Create Failed**
CAM_EVT_FACE_USER_UPDATE_FAILED	**Face User Update Failed**
CAM_EVT_FACE_USER_DELETE_FAILED	**Face User Delete Failed**
CAM_EVT_AI_ANALYSIS_CREATED	**AI Analysis Created**
CAM_EVT_AI_ANALYSIS_UPDATED	**AI Analysis Updated**
CAM_EVT_AI_ANALYSIS_DELETED	**AI Analysis Deleted**
CAM_EVT_AI_ANALYSIS_DELETE_STARTED	**AI Analysis Delete Started**

Tipos de registro	Descripción
CAM_EVT_AI_EVENT_SETTINGS_UPDATED	**AI Event Settings Updated**
CAM_EVT_PEOPLE_COUNT_RESET_ALL	**People Count Reset All**
CAM_EVT_PEOPLE_COUNT_RESET	**People Count Reset**
CAM_EVT_PEOPLE_COUNT_AUTO_RESET	**People Count Auto Reset**
CAM_EVT_AUDIO_CLIP_UPLOADED	**Audio Clip Uploaded**
CAM_EVT_AUDIO_CLIP_DELETED	**Audio Clip Deleted**
CAM_EVT_AUDIO_CLIP_PLAY	**Audio Clip Play**
CAM_EVT_AUDIO_CLIP_PLAYED	**Audio Clip Played**
CAM_EVT_AUDIO_CLIP_PLAY_FAILED	**Audio Clip Play Failed**
CAM_EVT_AUDIO_CLIP_API_PLAY	**Audio Clip API Play**
CAM_EVT_AUDIO_CLIP_API_STOP	**Audio Clip API Stop**
CAM_EVT_RELAY_SENT	**Relay command sent**
CAM_EVT_RELAY_FAILED	**Relay communication failed**
CAM_EVT_RELAY_KEEP_STARTED	**Relay keep started**
CAM_EVT_RELAY_KEEP_ENDED	**Relay keep ended**
CAM_EVT_RELAY_KEEP_REARM_FAILED	**Relay keep re-arm failed**
CAM_EVT_RELAY_OPENED	**Relay opened**
CAM_EVT_RELAY_LOCKED	**Relay locked**
CAM_EVT_RELAY_RELEASED	**Relay released**
CAM_EVT_RELAY_OPEN_REJECTED	**Relay open rejected**
CAM_EVT_RELAY_AUTO_CLOSED	**Relay auto-closed**
CAM_EVT_RELAY_STATE_RESTORED	**Relay state restored**
CAM_EVT_RELAY_UNLOCKED	**Relay unlocked**

Tipos de registro	Descripción
CAM_EVT_RELAY_IDLE_STATE_CHANGED	**Relay idle state changed**
CAM_EVT_RELAY_IDLE_STATE_APPLIED	**Relay idle state applied**
CAM_EVT_RELAY_OPEN_FAILED	**Relay open failed**
CAM_EVT_RELAY_LOCK_FAILED	**Relay lock failed**
CAM_EVT_RELAY_RELEASE_FAILED	**Relay release failed**
CAM_EVT_RELAY_AUTO_CLOSE_FAILED	**Relay auto-close failed**
CAM_EVT_RELAY_STATE_RESTORE_FAILED	**Relay state restore failed**
CAM_EVT_RELAY_UNLOCK_FAILED	**Relay unlock failed**
CAM_EVT_RELAY_IDLE_STATE_CHANGE_FAILED	**Relay idle state change failed**
CAM_EVT_RELAY_IDLE_STATE_APPLY_FAILED	**Relay idle state apply failed**
CAM_EVT_RELAY_TOKEN_MIGRATED	**Relay token migrated**
CAM_EVT_SCHEDULE_CREATED	**Schedule created**
CAM_EVT_SCHEDULE_UPDATED	**Schedule updated**
CAM_EVT_SCHEDULE_DELETED	**Schedule deleted**
CAM_EVT_SCHEDULE_LEGACY_MIGRATED	**Schedule data migrated**
CAM_EVT_ACCESS_DOOR_CREATED	**Door created**
CAM_EVT_ACCESS_DOOR_UPDATED	**Door updated**
CAM_EVT_ACCESS_DOOR_DELETED	**Door deleted**
CAM_EVT_ACCESS_DOOR_DELETE_STARTED	**Door delete started**
CAM_EVT_ACCESS_DOOR_DELETE_FAILED	**Door delete failed**
CAM_EVT_ACCESS_LEVEL_CREATED	**Access level created**
CAM_EVT_ACCESS_LEVEL_UPDATED	**Access level updated**
CAM_EVT_ACCESS_LEVEL_DELETED	**Access level deleted**

Tipos de registro	Descripción
CAM_EVT_ACCESS_MEMBERSHIP_UPDATED	**Access level membership updated**
CAM_EVT_ACCESS_POLICY_APPLY_STARTED	**Access policy apply started**
CAM_EVT_ACCESS_POLICY_APPLIED	**Access policy applied**
CAM_EVT_ACCESS_POLICY_APPLY_FAILED	**Access policy apply failed**
CAM_EVT_ACCESS_RUNTIME_RECOVERED	**Access runtime recovered**
CAM_EVT_ACCESS_RUNTIME_RECOVER_FAILED	**Access runtime recovery failed**
CAM_EVT_ACCESS_POLICY_REBUILT_ON_BOOT	**Access policy rebuilt on boot**
CAM_EVT_ACCESS_RUNTIME_DEGRADED	**Access runtime degraded**
CAM_EVT_ACCESS_DOOR_TRIGGER_CREATED	**Door trigger binding created**
CAM_EVT_ACCESS_DOOR_TRIGGER_UPDATED	**Door trigger binding updated**
CAM_EVT_ACCESS_DOOR_TRIGGER_DELETED	**Door trigger binding deleted**
CAM_EVT_ACCESS_DOOR_PASSED_UNIDENTIFIED	**Passage (unidentified)**
CAM_EVT_ACCESS_DOOR_UNLOCK_REQUESTED	**Door unlock requested**
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_DOOR_MODE	**Door access denied (door mode)**
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_UNIDENTIFIED	**Door access denied (unidentified)**
CAM_EVT_ACCESS_DOOR_ACCESS_GRANTED	**Door access granted**
CAM_EVT_ACCESS_DOOR_ACCESS_GRANTED_ALREADY_UNLOCKED	**Door access granted (already unlocked)**
CAM_EVT_ACCESS_DUAL_AUTH_PENDING	**Dual authentication pending**
CAM_EVT_ACCESS_DUAL_AUTH_TIMEOUT	**Dual authentication timed out**
CAM_EVT_ACCESS_DOOR_SCHEDULE_UNLOCKED	**Schedule unlock started**
CAM_EVT_ACCESS_DOOR_SCHEDULE_LOCKED	**Schedule lock started**
CAM_EVT_ACCESS_DOOR_SCHEDULE_RELEASED	**Schedule window released**
CAM_EVT_ACCESS_DOOR_HOLD_RELEASED	**Keep-unlock released**

Tipos de registro	Descripción
CAM_EVT_ACCESS_DOOR_RULE_ACTION_SUCCEEDED	**Door rule action succeeded**
CAM_EVT_ACCESS_DOOR_RULE_ACTION_FAILED	**Door rule action failed**
CAM_EVT_ACCESS_DOOR_RULE_CREATED	**Door rule created**
CAM_EVT_ACCESS_DOOR_RULE_UPDATED	**Door rule updated**
CAM_EVT_ACCESS_DOOR_RULE_DELETED	**Door rule deleted**
CAM_EVT_ACCESS_EXIT_BUTTON_UNLOCKED	**Exit button unlocked**
CAM_EVT_ACCESS_DOOR_EARLY_RELOCKED	**Door early relocked**
CAM_EVT_ACCESS_EXIT_BUTTON_UNLOCK_FAILED	**Exit button unlock failed**
CAM_EVT_ACCESS_DOOR_PASSED	**Authenticated passage**
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_ACCESS_LEVEL	**Door access denied (access level)**
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_TAILGATING	**Door access denied (tailgating)**
CAM_EVT_ACCESS_DOOR_UNLOCK_FAILED	**Door unlock failed**
CAM_EVT_ACCESS_DOOR_PASSED_AFTER_DENIED	**Passage after denial**
CAM_EVT_ACCESS_DOOR_RULE_ACTION_RETRYING	**Door rule action retrying**
CAM_EVT_ACCESS_DOOR_RULE_MUTATION_REJECTED	**Door rule change rejected**
CAM_EVT_HEATER_CONTROL_REQUESTED	**Heater control requested**
CAM_EVT_HEATER_ENABLED	**Heater enabled**
CAM_EVT_HEATER_DISABLED	**Heater disabled**
CAM_EVT_HEATER_AUTO_DISABLED	**Heater auto-disabled**
CAM_EVT_HEATER_CONTROL_FAILED	**Heater control failed**
CAM_EVT_HEATER_STATE_RECONCILED	**Heater state reconciled**
CAM_EVT_HEATER_BOOT_RECOVERED	**Heater boot recovered**
CAM_EVT_HEATER_BOOT_RECOVERY_FAILED	**Heater boot recovery failed**

Tipos de registro	Descripción
CAM_EVT_HEATER_FAULT_DISABLED	**Heater disabled by fault**
CAM_EVT_INPUT_IDLE_STATE_CHANGED	**Input idle state changed**
CAM_EVT_INPUT_IDLE_STATE_CHANGE_FAILED	**Input idle state change failed**
CAM_SYS_NETWORK_CHANGE	**Network Settings Changed**
CAM_SYS_NETWORK_DHCP_FALLBACK	**DHCP Fallback to Link-local**
CAM_SYS_DATETIME_CHANGE	**Date/Time Settings Changed**
CAM_SYS_NTP_SYNC_FAILED	**NTP Sync Failed**
CAM_SYS_FIRMWARE_UPGRADE	**Firmware Upgrade**
CAM_SYS_SYSTEM_STARTED	**Web Server Started**
CAM_SYS_FACTORY_RESET	**Factory Reset**
CAM_SYS_CONFIG_RESET	**Config Reset**
CAM_SYS_SYSTEM_REBOOT	**System Reboot**
CAM_SYS_CLUE_ENABLED	**CLUe Enabled**
CAM_SYS_CLUE_DISABLED	**CLUe Disabled**
CAM_SYS_CLUE_ENABLE_FAILED	**CLUe Enable Failed**
CAM_SYS_CLUE_USER_SYNC_CHANGED	**CLUe user sync changed**
CAM_SYS_CLUE_TUNNEL_CHANGED	**CLUe tunnel changed**
CAM_SYS_CONSENT_ENROLLMENT_CHANGED	**Consent Enrollment Changed**
CAM_SYS_CONSENT_ANALYTICS_CHANGED	**Consent Analytics Changed**
CAM_SYS_AI_SETTINGS_CHANGED	**AI Settings Changed**
CAM_SYS_AI_LOAD_FAILED	**AI Load Failed**
CAM_SYS_SECURE_TAMPER_CHANGED	**Secure Tamper Settings Changed**
CAM_SYS_TUNNEL_MODE_CHANGED	**Tunnel mode changed**

Tipos de registro	Descripción
CAM_SYS_TUNNEL_SETTING_UPDATED	**Tunnel setting updated**
CAM_SYS_WEBRTC_SESSION_START	**WebRTC session started**
CAM_SYS_WEBRTC_SESSION_END	**WebRTC session ended**
CAM_SYS_CRYPTO_KEYGEN_FAILED	**Crypto key generation failed**
CAM_SYS_CRYPTO_OP_FAILED	**Crypto operation failed**
CAM_SYS_SLAVE_CONNECTED	**RS485 slave connected**
CAM_SYS_SLAVE_DISCONNECTED	**RS485 slave disconnected**
CAM_SYS_RS485_SLAVE_FW_UPDATE_SUCCEEDED	**Slave firmware update succeeded**
CAM_SYS_RS485_SLAVE_FW_UPDATE_FAILED	**Slave firmware update failed**
CAM_SYS_ONVIF_MODE_CHANGED	**ONVIF mode changed**
CAM_SYS_ONVIF_HTTP_PROXY_FAILED	**ONVIF HTTP proxy failed**
CAM_SYS_API_OPERATION_FAILED	**API operation failed**
CAM_SYS_API_COMPLETION_UNCONFIRMED	**API completion unconfirmed**
CAM_SYS_API_REQUEST_REJECTED	**API request rejected**
CAM_ACC_LOGIN	**Login**
CAM_ACC_LOGOUT	**Logout**
CAM_ACC_TOKEN_REFRESH	**Token Refreshed**
CAM_ACC_PASSWORD_CHANGE	**Password Changed**
CAM_ACC_AUTH_FAILURE	**Authentication Failure**
CAM_ACC_REFRESH_TOKEN_REUSE	**Refresh Token Reuse Detected**
CAM_ACC_SESSION_INVALIDATED	**Session Invalidated**
CAM_ACC_RATE_LIMIT_EXCEEDED	**Rate Limit Exceeded**
CAM_ACC_FORBIDDEN_ACCESS	**Forbidden Access**

Tipos de registro	Descripción
CAM_ACC_PASSWORD_SETUP	**Password Setup**
CAM_ACC_ACCOUNT_LOCKED	**Account Locked**
CAM_ACC_SESSION_EXPIRED	**Session Expired**
CAM_ACC_ACCOUNT_CREATED	**Account Created**
CAM_ACC_ACCOUNT_UPDATED	**Account Updated**
CAM_ACC_ACCOUNT_DELETED	**Account Deleted**
CAM_ACC_ACCOUNT_DISABLED	**Account Disabled**
CAM_ACC_SESSION_KICKED	**Session Force Terminated**
CAM_ACC_LOGIN_FAILED	**Login Failed**
CAM_ACC_PERMISSION_DENIED	**Permission denied**
CAM_ACC_SESSION_LIMIT_REJECTED	**Session limit rejected**
CAM_ACC_ACCOUNT_CREATE_FAILED	**Account create failed**

Apéndices

Incluye avisos legales contenidos en el producto.

Descargos de responsabilidad

- La información de este sitio web se proporciona en relación con los productos de Suprema.
- El derecho de uso se reconoce únicamente para los productos de Suprema incluidos en los términos y condiciones de uso o venta de dichos productos garantizados por Suprema. Este sitio web no otorga ninguna licencia, expresa o implícita, por impedimento legal ni de ningún otro tipo, sobre ninguna propiedad intelectual.
- Salvo lo expresamente establecido en un acuerdo entre usted y Suprema, Suprema no asume ninguna responsabilidad y rechaza toda garantía, expresa o implícita, incluidas, entre otras, las relativas a la idoneidad para un fin particular, la comerciabilidad o la no infracción.
- Todas las garantías quedan ANULADAS si los productos de Suprema han sido: 1) instalados incorrectamente o si los números de serie, la fecha de garantía o las etiquetas de control de calidad del hardware han sido alterados o retirados; 2) utilizados de una manera distinta a la autorizada por Suprema; 3) modificados, alterados o reparados por un tercero que no sea Suprema o un tercero autorizado por Suprema; o 4) operados o mantenidos en condiciones ambientales inadecuadas.
- Los productos de Suprema no están destinados a usos médicos, de salvamento, de soporte vital ni a otras aplicaciones en las que la falla del producto de Suprema pudiera ocasionar lesiones personales o la muerte. Si compra o utiliza productos de Suprema para cualquiera de estas aplicaciones no previstas ni autorizadas, deberá indemnizar y eximir de responsabilidad a Suprema y a sus directores, empleados, subsidiarias, afiliadas y distribuidores por todos los reclamos, costos, daños y gastos, incluidos los honorarios razonables de abogados, derivados directa o indirectamente de cualquier reclamo por lesiones personales o muerte asociado con dicho uso no previsto o no autorizado, incluso si el reclamo alega que Suprema fue negligente en el diseño o la fabricación de la pieza.
- Suprema se reserva el derecho de realizar cambios en las especificaciones y descripciones de los productos en cualquier momento y sin previo aviso para mejorar la confiabilidad, la función o el diseño.
- La información personal, en forma de mensajes de autenticación y otra información relacionada, puede almacenarse en los productos de Suprema durante su uso. Suprema no se hace responsable de ninguna información, incluida la información personal, almacenada dentro de los productos de Suprema que no esté bajo el control directo de Suprema o según lo establecido en los términos y condiciones correspondientes. Cuando se utilice cualquier información almacenada, incluida la información personal, es responsabilidad de los usuarios del producto cumplir con la legislación nacional (como el RGPD) y garantizar su manipulación y tratamiento adecuados.
- No debe confiar en la ausencia o las características de ninguna función o instrucción marcada como "reservada" o "indefinida". Suprema las reserva para su definición futura y no tendrá ninguna responsabilidad por conflictos o incompatibilidades derivados de cambios posteriores en ellas.
- Salvo que se disponga expresamente en el presente documento y en la medida máxima permitida por la ley, los productos de Suprema se venden "tal cual".
- Comuníquese con la oficina de ventas local de Suprema o con su distribuidor para obtener las especificaciones más recientes y antes de realizar su pedido.

Aviso de derechos de autor

Los derechos de autor de este sitio web pertenecen a Suprema. Los derechos sobre otros nombres de productos, marcas comerciales y marcas registradas pertenecen a las personas u organizaciones propietarias.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

Para obtener más información sobre las sucursales globales de Suprema,
visite la página web a continuación escaneando el código QR.
http://www.supremainc.com/en/about/contact-us.asp

© 2026 Suprema Inc. Suprema y los números y los nombres que identifican productos mencionados en este documento son marcas comerciales registradas de Suprema, Inc. Todas las marcas y los nombres de productos que no pertenecen a Suprema son marcas comerciales o marcas comerciales registradas de sus respectivas compañías. La apariencia del producto, el estado de la estructura o las especificaciones están sujetas a cambio sin previo aviso.